Manual do usuário

AWS Acesso verificado

AWS Acesso verificado: Manual do usuário

Table of Contents

O que Acesso Verificado pela AWSé

Com Acesso Verificado pela AWS, você pode fornecer acesso seguro aos seus aplicativos sem exigir o uso de uma rede privada virtual (VPN). O Acesso Verificado avalia cada solicitação de aplicativo e ajuda a garantir que os usuários possam acessar cada aplicativo somente quando atenderem aos requisitos de segurança especificados.

Benefícios do Acesso Verificado

- Postura de segurança aprimorada: um modelo de segurança tradicional avalia o acesso uma vez e concede ao usuário acesso a todos os aplicativos. O Acesso Verificado avalia cada solicitação de acesso ao aplicativo em tempo real. Isso dificulta a migração de agentes mal-intencionados de um aplicativo para outro.
- Integração com serviços de segurança — O Verified Access se integra aos serviços de gerenciamento de identidade e dispositivos, incluindo serviços de terceiros AWS e de terceiros. Usando dados desses serviços, o Acesso Verificado analisa a confiabilidade dos usuários e dispositivos em relação a um conjunto de requisitos de segurança e determina se o usuário deve ter acesso a um aplicativo.
- Experiência de usuário aprimorada — O acesso verificado elimina a necessidade de os usuários usarem um VPN para acessar seus aplicativos. Isso ajuda a reduzir o número de casos de suporte decorrentes de problemas VPN relacionados.
- Solução de problemas e auditorias simplificadas: o Acesso Verificado registra todas as tentativas de acesso, fornecendo visibilidade centralizada do acesso aos aplicativos, para ajudá-lo a responder rapidamente a incidentes de segurança e solicitações de auditoria.

Acessar o Acesso Verificado pela

Você pode trabalhar com o Acesso Verificado usando qualquer uma das seguintes interfaces:

- AWS Management Console: fornece uma interface de usuário baseada na Web que pode ser usada para criar e gerenciar recursos do Acesso Verificado. Faça login no AWS Management Console e abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
- AWS Command Line Interface (AWS CLI) — Fornece comandos para um amplo conjunto de Serviços da AWS, incluindo Acesso Verificado pela AWS. O AWS CLI é compatível com Windows, macOS e Linux. Para obter o AWS CLI, consulte AWS Command Line Interface.

- AWS SDKs— Forneça um idioma específicoAPIs. Eles AWS SDKs cuidam de muitos detalhes da conexão, como calcular assinaturas e lidar com erros e tentativas de solicitação. Para obter mais informações, consulte AWS SDKs.
- Consulta API — fornece API ações de baixo nível que você chama usando HTTPS solicitações. Usar a Consulta API é a forma mais direta de acessar o Acesso Verificado. No entanto, ela exige que a aplicação trate detalhes de baixo nível, como gerar o hash para assinar a solicitação e tratar erros. Para obter mais informações, consulte Ações de acesso verificado na Amazon EC2 API Reference.

Este guia descreve como usar o AWS Management Console para criar, acessar e gerenciar recursos de acesso verificado.

Definição de preço

Você será cobrado por hora por cada aplicativo no Acesso Verificado e pela quantidade de dados processada pelo Acesso Verificado. Para obter mais informações, consulte Definição de preço do Acesso Verificado pela AWS.

Como funciona o Acesso Verificado

Acesso Verificado pela AWS avalia cada solicitação de aplicativo de seus usuários e permite o acesso com base em:

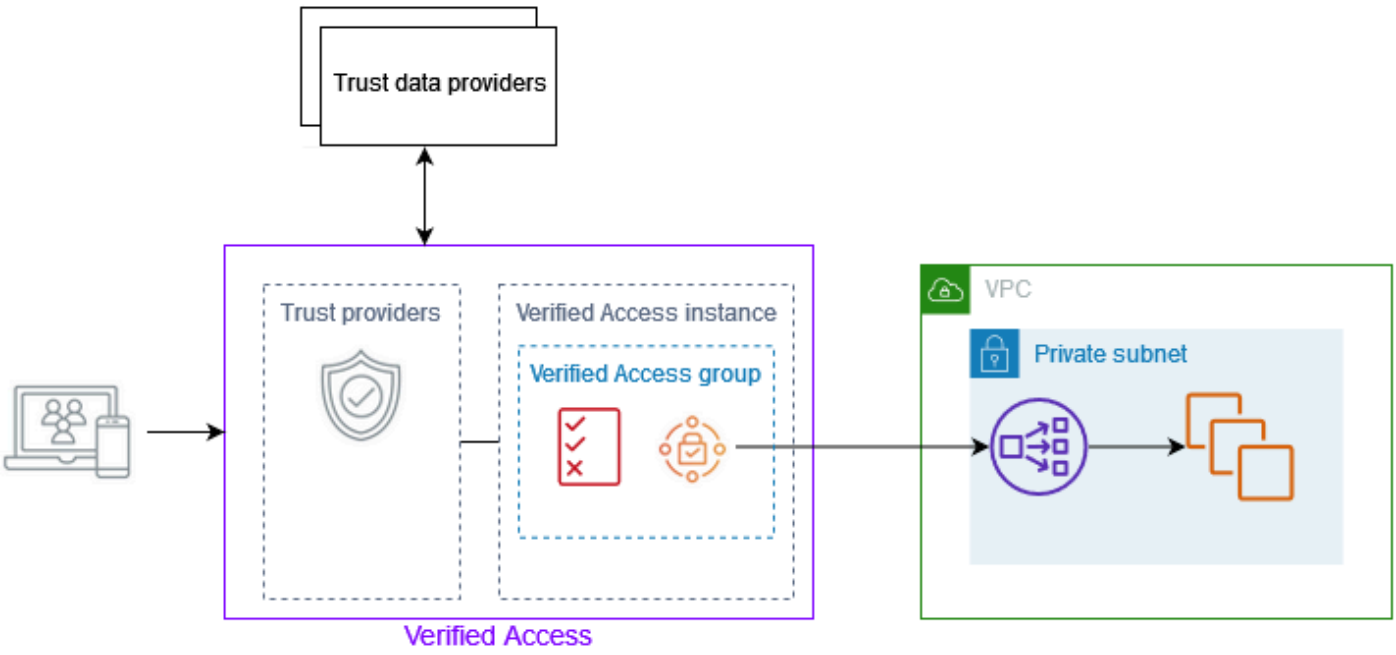
- Dados confiáveis enviados pelo provedor de confiança escolhido (de AWS ou de terceiros).
- Políticas de acesso que você cria no Acesso Verificado.

Quando um usuário tenta acessar um aplicativo, o Acesso Verificado obtém seus dados do provedor confiável e os avalia em relação às políticas que você definiu para o aplicativo. O Acesso Verificado concede acesso ao aplicativo solicitado somente se o usuário atender aos requisitos de segurança especificados. Todas as solicitações de aplicativos são negadas por padrão, até que uma política seja definida.

Além disso, o Acesso Verificado registra todas as tentativas de acesso, para ajudar você a responder rapidamente a incidentes de segurança e solicitações de auditoria.

Principais componentes do Acesso Verificado

O seguinte diagrama fornece uma visão geral de alto nível sobre como o Acesso Verificado funciona. Os usuários enviam solicitações para acessar um aplicativo. O Acesso Verificado avalia a solicitação em relação à política de acesso do grupo e a qualquer política de endpoint específica do aplicativo. Se o acesso for permitido, a solicitação será enviada para o aplicativo por meio do endpoint.



- Instâncias de Acesso Verificado: uma instância avalia as solicitações de aplicativos e concede acesso somente quando seus requisitos de segurança são atendidos.
- Endpoints de Acesso Verificado: cada endpoint representa um aplicativo. Você pode criar um endpoint de balanceador de carga ou um endpoint de interface de rede.
- Grupo de Acesso Verificado: uma coleção de endpoints de Acesso Verificado. Recomendamos que você agrupe os endpoints para aplicativos com requisitos de segurança semelhantes para simplificar a administração de políticas. Por exemplo, você pode agrupar os endpoints de todos os seus aplicativos de vendas.
- Políticas de acesso: um conjunto de regras definidas pelo usuário que determinam se o acesso a um aplicativo deve ser permitido ou negado. Você pode especificar uma combinação de fatores, incluindo identidade do usuário e estado de segurança do dispositivo. Você cria uma política de acesso de grupo para cada grupo de Acesso Verificado, que é herdada por todos os endpoints do grupo. Opcionalmente, você pode criar políticas específicas do aplicativo e anexá-las a endpoints específicos.
- Provedores confiáveis: um serviço que gerencia as identidades dos usuários ou o estado de segurança do dispositivo. O Verified Access funciona com provedores AWS fiduciários e terceirizados. Você deve anexar pelo menos um provedor de confiança a cada instância de Acesso Verificado. Você pode anexar um único provedor de confiança de identidade e vários provedores de confiança de dispositivos a cada instância de Acesso Verificado.

- Dados de confiança: os dados relacionados à segurança de usuários ou dispositivos que seu provedor confiável envia para o Acesso Verificado. Também conhecido como reivindicações do usuário ou contexto de confiança. Por exemplo, o endereço de e-mail de um usuário ou a versão do sistema operacional de um dispositivo. O Acesso Verificado avalia esses dados em relação às suas políticas de acesso ao receber cada solicitação para acessar um aplicativo.

Tutorial: Comece com o acesso verificado

Use este tutorial para começar Acesso Verificado pela AWS. Você aprenderá a criar e configurar recursos de Acesso Verificado.

Como parte deste tutorial, você adicionará um aplicativo ao Acesso Verificado. Ao final do tutorial, usuários específicos poderão acessar esse aplicativo pela internet, sem usarVPN.

> **Note**
>
> Este tutorial não demonstra a integração com seu provedor de confiança baseado em dispositivos. Em vez disso, trabalhamos apenas com um provedor de confiança baseado em identidade.

Tarefas

Pré-requisitos do tutorial de acesso verificado

A seguir estão os pré-requisitos para concluir este tutorial:

- A disponibilidade de dois Contas da AWS. Uma conta hospeda seu aplicativo de destino e os recursos de acesso verificado são criados na outra conta.
- AWS IAM Identity Center ativado no em Região da AWS que você está trabalhando. Em seguida, você pode usar o IAM Identity Center como um provedor confiável com acesso verificado. Para obter mais informações, consulte Habilitar o IAM Identity Center no Guia AWS IAM Identity Center do usuário.
- Um domínio público hospedado e as permissões necessárias para atualizar DNS os registros do domínio.
- Um aplicativo executado por trás de um balanceador de carga interno em um Conta da AWS. O exemplo de nome de domínio do aplicativo que usaremos é `www.myapp.example.com`.
- Uma IAM política que tem todas as permissões necessárias para criar uma Acesso Verificado pela AWS instância indicada aquiPolítica para criar instâncias de Acesso Verificado.

Etapa 1: Criar uma instância do Acesso Verificado

Use o procedimento a seguir para criar uma instância do Acesso Verificado.

Para criar uma instância do Acesso Verificado

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de VPC navegação da Amazon, escolha Instâncias de acesso verificado e, em seguida, Criar instância de acesso verificado.
3. (Opcional) Em Nome e Descrição, insira um nome e uma descrição para a instância do Acesso Verificado.
4. Para Trust provider, mantenha a opção padrão.
5. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
6. Escolha Criar instância de Acesso Verificado.

Etapa 2: Configurar um provedor confiável de acesso verificado

Você pode se configurar AWS IAM Identity Center como seu provedor de confiança.

Para criar um provedor confiável do IAM Identity Center

1. No painel de VPC navegação da Amazon, escolha Provedores de confiança de acesso verificado e, em seguida, Criar provedor confiável de acesso verificado.
2. (Opcional) Em Tag de nome e Descrição, insira um nome e uma descrição para o provedor confiável de Acesso Verificado.
3. Insira um identificador personalizado para usar posteriormente ao trabalhar com regras de política para o nome de referência da política. Por exemplo, insira: **`idc`**
4. Em Tipo de provedor confiável, selecione Provedor de confiança do usuário.
5. Em Tipo de provedor de confiança do usuário, selecione IAMIdentity Center.
6. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
7. Escolha Criar provedor confiável de Acesso Verificado.

Etapa 3: anexar seu provedor de confiança à instância de acesso verificado

Agora que você configurou um provedor de confiança, pode anexá-lo à instância de acesso verificado que você criou anteriormente. Use o procedimento a seguir para associar o provedor de confiança à sua instância do Acesso Verificado.

Para anexar um provedor de confiança à sua instância

1. No painel de VPC navegação da Amazon, escolha Instâncias de acesso verificado.
2. Selecione sua instância.
3. Escolha Ações, Anexar provedor confiável de Acesso Verificado.
4. Para provedor confiável de Acesso Verificado, escolha seu provedor de confiança.
5. Escolha Anexar provedor confiável de Acesso Verificado.

Etapa 4: criar um grupo de acesso verificado

Nesta etapa, você cria um grupo que usará como endpoint na Etapa 5.

Para criar um grupo do Acesso Verificado

1. No painel de VPC navegação da Amazon, escolha Grupos de acesso verificado e, em seguida, Criar grupo de acesso verificado.
2. (Opcional) Em Tag de nome e Descrição, insira um nome e uma descrição para o grupo.
3. Para instância de Acesso Verificado, escolha sua instância de Acesso Verificado.
4. Para definição de política, mantenha isso em branco. Você vai criar uma política mais adiante neste tutorial.
5. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
6. Escolha Criar grupo de Acesso Verificado.

Etapa 5: compartilhe seu grupo de acesso verificado por meio de AWS Resource Access Manager

Nesta etapa, você compartilha o grupo que acabou de criar com o Conta da AWS no qual seu aplicativo de destino está sendo executado. Para compartilhar um grupo de Acesso Verificado, é necessário adicioná-lo a um compartilhamento de recursos. Caso você não tenha um compartilhamento de recursos, primeiro será necessário criar um.

Se você faz parte de uma organização e o compartilhamento dentro da sua organização está ativado, os consumidores da sua organização recebem automaticamente acesso ao grupo compartilhado de Acesso Verificado. AWS Organizations Caso contrário, os consumidores receberão um convite para participar do compartilhamento de recursos e acesso ao Acesso Verificado compartilhado depois de aceitar o convite.

Siga as etapas em Criar um compartilhamento de recursos no Manual do usuário do AWS RAM . Em Selecionar tipo de recurso, escolha Grupo do Acesso Verificado e marque a caixa de seleção do seu grupo do Acesso Verificado.

Para obter mais informações, consulte Conceitos básicos no Guia do usuário do AWS RAM .

Etapa 6: adicione seu aplicativo criando um endpoint de acesso verificado

Use os procedimentos a seguir para criar um endpoint de acesso verificado. Essa etapa pressupõe que você tenha um aplicativo em execução por trás de um balanceador de carga interno do Elastic Load Balancing.

Para criar um endpoint do Acesso Verificado

1. No painel de VPC navegação da Amazon, escolha Endpoints de acesso verificado e, em seguida, Create Verified Access endpoint.
2. (Opcional) Em Tag de nome e Descrição, insira um nome e uma descrição para o endpoint.
3. Para Grupo de Acesso Verificado, escolha seu grupo de Acesso Verificado.
4. Para obter detalhes do aplicativo faça o seguinte:
    a. Em Domínio do aplicativo, insira um DNS nome para seu aplicativo.
    b. Em Certificado de domínio ARN, selecione o Amazon Resource Name (ARN) do seu TLS certificado público.
5. Em Detalhes do endpoint, faça o seguinte:
    a. Em Tipo de anexo, escolha VPC.
    b. Em Grupos de segurança, selecione o grupo de segurança a ser associado ao endpoint.
    c. Em Prefixo de domínio do Endpoint, insira um identificador personalizado. Isso será anexado ao DNS nome que o Acesso Verificado gera. Para este exemplo, usaremos **`my-ava-app`**.
    d. Em Tipo de endpoint escolha balanceador de carga.
    e. Em Protocolo, selecione HTTPSou HTTP. Isso depende da configuração do seu balanceador de carga.
    f. Em Porta, digite o número da porta. Isso depende da configuração do seu balanceador de carga.
    g. Em Balanceador de carga ARN, escolha seu balanceador de carga.
    h. Em Sub-redes, selecione as sub-redes associadas ao seu balanceador de carga.
6. Para definição de política, não insira uma política no momento. Abordaremos isso posteriormente no tutorial.

7. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
8. Escolha Criar endpoint de Acesso Verificado.

Etapa 7: DNS Definir as configurações do endpoint de acesso verificado

Nesta etapa, você mapeia o nome de domínio do seu aplicativo (por exemplo, www.myapp.example.com) para o nome de domínio do seu endpoint de Acesso Verificado. Para concluir o DNS mapeamento, crie um registro de nome canônico (CNAME) com seu DNS provedor. Depois de criar o CNAME registro, todas as solicitações dos usuários ao seu aplicativo serão enviadas para o Acesso Verificado.

Para obter o nome de domínio do endpoint.

1. No painel de VPC navegação da Amazon, escolha Endpoints de acesso verificado.
2. Selecione o endpoint que você criou anteriormente.
3. Escolha a guia Detalhes para o endpoint.
4. Em Domínio do endpoint, copie o domínio do endpoint.

Neste tutorial, o nome de domínio do endpoint será `my-ava-app.edge-1a2b3c4d5e6f7g.vai-1a2b3c4d5e6f7g.prod.verified-access.us-west-2.amazonaws.com`.

Crie um CNAME registro com seu DNS provedor:

Nome de registro	Tipo	Valor
www.myapp.example.com	CNAME	my-ava-app.edge-1a 2b3c4d5e6f7g.vai-1 a2b3c4d5e6f7g.prod. verified-access.us-west-2.amazonaws. com

Etapa 8: testar a conectividade com o aplicativo que você adicionou ao Acesso verificado

Agora você pode testar a conectividade com seu aplicativo. Insira o nome de domínio do seu aplicativo em seu navegador da web. O comportamento padrão das políticas do Acesso Verificado é negar todas as solicitações. Como ainda não implementamos uma política que permita o acesso de qualquer pessoa, todas as solicitações devem ser negadas.

Etapa 9: Configurar uma política de acesso verificado em nível de grupo de acesso

Use o procedimento a seguir para modificar o grupo de Acesso Verificado e configurar uma política de acesso que permita a conectividade com seu aplicativo. Os detalhes da política dependerão dos usuários e grupos configurados no IAM Identity Center. Para obter informações sobre a criação de uma política, consulte Políticas do Acesso Verificado.

Para modificar um grupo de Acesso Verificado

1. No painel de VPC navegação da Amazon, escolha Grupos de acesso verificado.
2. Selecione seu grupo.
3. Escolha Ações, Modificar política de grupo de Acesso Verificado.
4. Insira a política.
5. Escolha Modificar política de grupo de Acesso Verificado.

Etapa 10: testar novamente a conectividade com o aplicativo que você adicionou ao Acesso Verificado

Agora que sua política de grupo está em vigor, você pode acessar seu aplicativo. Insira o nome de domínio do seu aplicativo em seu navegador da web. A solicitação deve ser permitida e você deve ser redirecionado para o aplicativo.

Limpe os recursos de acesso verificado que você criou

Depois de concluir o teste, siga a etapa abaixo para excluir os recursos que foram criados.

Para excluir os recursos de Acesso Verificado criados com este tutorial

1. No painel de VPC navegação da Amazon, escolha Endpoints de acesso verificado. Selecione o endpoint que deseja remover. Escolha Ações, Excluir endpoint de Acesso Verificado.
2. No painel de navegação, escolha Grupos de Acesso Verificado. Selecione o grupo que deseja remover. Escolha Ações, Excluir grupo de Acesso Verificado. Observação: talvez seja necessário aguardar alguns minutos até que o processo de exclusão do endpoint seja concluído.
3. No painel de VPC navegação da Amazon, escolha Instâncias de acesso verificado. Selecione a instância que você criou para este tutorial. Escolha Ações, Desanexe o provedor confiável de Acesso Verificado. Selecione o provedor de confiança na lista suspensa e escolha Desanexar provedor confiável de Acesso Verificado.
4. No painel de VPC navegação da Amazon, escolha Provedores confiáveis de acesso verificado. Selecione o provedor de confiança que você criou para este tutorial. Escolha Ações, Excluir provedor confiável de Acesso Verificado.
5. No painel de VPC navegação da Amazon, escolha Instâncias de acesso verificado. Selecione a instância que você criou para este tutorial. Escolha Ações, Excluir instância de Acesso Verificado.

Instâncias de Acesso Verificado

Uma Acesso Verificado pela AWS instância é um AWS recurso que ajuda você a organizar seus provedores de confiança e grupos de acesso verificado. Uma instância avalia as solicitações de aplicativos e concede acesso somente quando seus requisitos de segurança são atendidos.

Tópicos

Crie e gerencie uma instância de acesso verificado

Você usa uma instância de acesso verificado para organizar seus provedores de confiança e grupos de acesso verificado. Use os procedimentos a seguir para criar uma instância de acesso verificado e, em seguida, anexar um provedor confiável ao Acesso verificado ou desanexar um provedor confiável do Acesso verificado.

Tópicos

Criar uma instância do Acesso Verificado

Use o procedimento a seguir para criar uma instância do Acesso Verificado.

Para criar uma instância do Acesso Verificado

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Instâncias de Acesso Verificado e, em seguida, Criar instância de Acesso Verificado.
3. (Opcional) Em Nome e Descrição, insira um nome e uma descrição para a instância do Acesso Verificado.

4. (Opcional) Escolha ativar para os Padrões Federais de Processo de Informações (FIPS) se você precisar que o Acesso Verificado esteja FIPS em conformidade.
5. (Opcional) Em Provedor confiável, escolha um provedor confiável para anexar à instância de Acesso Verificado.
6. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
7. Escolha Criar instância de Acesso Verificado.

Anexar um provedor de confiança a uma instância de acesso verificado

Use o procedimento a seguir para associar um provedor de confiança a uma instância do Acesso Verificado.

Para anexar um provedor de confiança a uma instância do Acesso Verificado

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do Acesso Verificado.
3. Selecione a instância.
4. Escolha Ações, Anexar provedor confiável de Acesso Verificado.
5. Para provedor confiável de Acesso Verificado, escolha um provedor confiável.
6. Escolha Anexar provedor confiável de Acesso Verificado.

Separar um provedor confiável de uma instância de acesso verificado

Use o procedimento a seguir para desvincular um provedor de confiança de uma instância do Acesso Verificado.

Para desvincular um provedor de confiança de uma instância do Acesso Verificado

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do Acesso Verificado.
3. Selecione a instância.
4. Escolha Ações, Desanexe o provedor confiável de Acesso Verificado.
5. Para provedor confiável de Acesso Verificado, escolha o provedor confiável.
6. Escolha Desanexar provedor confiável de Acesso Verificado.

Excluir uma instância do Acesso Verificado

Quando não precisar mais de uma instância do Acesso Verificado, você poderá excluí-la. Antes de excluir uma instância, você deve remover todos os provedores de confiança ou grupos de Acesso Verificado associados.

Como excluir uma instância do Acesso Verificado

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do Acesso Verificado.
3. Selecione a instância de Acesso Verificado.
4. Escolha Ações, Excluir instância de Acesso Verificado.
5. Quando a confirmação for solicitada, insira **`delete`** e escolha Excluir.

Integre o acesso verificado com AWS WAF

Além das regras de autenticação e autorização impostas pelo Acesso Verificado, talvez você também queira aplicar a proteção de perímetro. Isso pode ajudar você a proteger seus aplicativos contra ameaças adicionais. Você pode fazer isso AWS WAF integrando-se à sua implantação do Verified Access. AWS WAF é um firewall de aplicativo web que permite monitorar as solicitações HTTP (S) que são encaminhadas para seus recursos protegidos de aplicativos web. Para obter mais informações sobre AWS WAF, consulte AWS WAFo Guia do AWS WAF desenvolvedor.

Você pode se integrar ao Acesso Verificado AWS WAF associando uma lista de controle de acesso à AWS WAF web (ACL) a uma instância de Acesso Verificado. Uma web ACL é um AWS WAF recurso que oferece controle refinado sobre todas as HTTP (S) solicitações da web às quais seu recurso protegido responde. Enquanto a solicitação de AWS WAF associação ou desassociação está sendo processada, o status de qualquer endpoint de acesso verificado anexado à instância é mostrado como. `updating` Depois que a solicitação for concluída, o status retornará a `active`. Você pode visualizar o status no AWS Management Console ou descrevendo o endpoint com o. AWS CLI

> **Note**
>
> Você também pode usar o AWS WAF console ou API realizar essa integração. Você precisará do Amazon Resource Name (ARN) da sua instância de acesso verificado. Você pode construir isso ARN usando o seguinte formato:`arn:`

```
${Partition}:ec2:${Region}:${Account}:verified-access-instance/
${VerifiedAccessInstanceId}.
```

Tópicos

- IAMpermissões necessárias para integrar o Acesso Verificado com AWS WAF
- Associar uma AWS WAF web ACL
- Verifique o status da AWS WAF integração
- Desassociar uma web AWS WAF ACL

IAMpermissões necessárias para integrar o Acesso Verificado com AWS WAF

A integração AWS WAF com o Acesso Verificado inclui ações somente com permissão que não correspondem diretamente a uma operação. API Essas ações são indicadas na AWS Identity and Access Management Referência de autorização de serviço com `[permission only]`. Consulte Ações, recursos e chaves de condição para a Amazon EC2 na Referência de autorização de serviço.

Para trabalhar com uma webACL, seu AWS Identity and Access Management diretor deve ter as seguintes permissões.

- `ec2:AssociateVerifiedAccessInstanceWebAcl`
- `ec2:DisassociateVerifiedAccessInstanceWebAcl`
- `ec2:DescribeVerifiedAccessInstanceWebAclAssociations`
- `ec2:GetVerifiedAccessInstanceWebAcl`

Associar uma AWS WAF web ACL

As etapas a seguir demonstram como associar uma lista de controle de acesso à AWS WAF web (ACL) a uma instância de acesso verificado usando AWS Management Console o.

> **Tip**
>
> Você precisará ter uma AWS WAF web existente ACL para concluir o procedimento abaixo. Para obter mais informações sobre a Web, ACLs consulte Listas de controle de acesso à Web no Guia do AWS WAF Desenvolvedor.

Para associar uma AWS WAF web ACL a uma instância de acesso verificado

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do Acesso Verificado.
3. Selecione a instância de Acesso Verificado.
4. Selecione a guia Integrações.
5. Escolha Ações e, em seguida, Associar Web ACL.
6. Em Web ACL, escolha uma Web existente eACL, em seguida, escolha Associar Web ACL.

Você também pode usar o AWS Management Console for AWS WAF para realizar essa tarefa. Para obter mais informações, consulte Associar ou desassociar uma web ACL a um AWS recurso no Guia do AWS WAF desenvolvedor.

Verifique o status da AWS WAF integração

Você pode verificar se uma lista de controle de acesso à AWS WAF web (ACL) está associada a uma instância de acesso verificado ou não usando AWS Management Console o.

Para ver o status da AWS WAF integração com uma instância de acesso verificado

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do Acesso Verificado.
3. Selecione a instância de Acesso Verificado.
4. Selecione a guia Integrações.
5. Verifique os detalhes listados em Status de WAF integração. O status será mostrado como Associado ou Não associado, junto com o ACL identificador da web, se estiver no estado Associado.

Desassociar uma web AWS WAF ACL

As etapas a seguir demonstram como desassociar uma lista de controle de acesso à AWS WAF web (ACL) com uma instância de acesso verificado usando o. AWS Management Console

Para desassociar uma AWS WAF web ACL de uma instância de acesso verificado

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do Acesso Verificado.
3. Selecione a instância de Acesso Verificado.
4. Selecione a guia Integrações.
5. Escolha Ações e, em seguida, Desassociar Web ACL.
6. Confirme escolhendo Disassociate Web ACL.

Você também pode usar o AWS Management Console for AWS WAF para realizar essa tarefa. Para obter mais informações, consulte Associar ou desassociar uma web ACL a um AWS recurso no Guia do AWS WAF desenvolvedor.

FIPSconformidade com o Verified Access

O Federal Information Processing Standard (FIPS) é um padrão do governo dos EUA e do Canadá que especifica requisitos de segurança para módulos criptográficos que protegem informações confidenciais. Acesso Verificado pela AWS fornece a opção de configurar seu ambiente para aderir à FIPS Publicação 140-2. FIPSa conformidade com o Acesso Verificado está disponível nas seguintes AWS regiões:

- Leste dos EUA (Ohio)
- Leste dos EUA (N. da Virgínia)
- Oeste dos EUA (N. da Califórnia)
- Oeste dos EUA (Oregon)
- Canadá (Central)
- AWS GovCloud (US) Oeste
- AWS GovCloud (US) Leste

Esta página mostra como configurar um ambiente novo ou existente de Acesso Verificado para ser FIPS compatível.

Tópicos

Configurar um ambiente existente de acesso verificado para fins de FIPS conformidade

Se você tiver um ambiente de acesso verificado existente e quiser configurá-lo para ser FIPS compatível, alguns dos recursos precisarão ser excluídos e recriados para ativar FIPS a conformidade.

Para reconfigurar um Acesso Verificado pela AWS ambiente existente para ser FIPS compatível, siga as etapas abaixo.

1. Exclua seus endpoints, grupos e instância originais do Acesso Verificado. Seus provedores de confiança configurados podem ser reutilizados.
2. Crie uma instância de acesso verificado, certificando-se de ativar os padrões federais de processo de informações (FIPS) durante a criação. Além disso, durante a criação, anexe o provedor confiável de Acesso Verificado que você deseja usar, selecionando-o na lista suspensa.
3. Crie um grupo de Acesso Verificado. Durante a criação do grupo, você o associa à instância de Acesso Verificado recém-criada.
4. Crie um ou mais Endpoints de Acesso Verificado. Durante a criação dos seus endpoints, você os associa ao grupo criado na etapa anterior.

Configure um novo ambiente de acesso verificado para fins de FIPS conformidade

Para configurar um novo Acesso Verificado pela AWS ambiente FIPS compatível, siga as etapas abaixo.

1. Configure um provedor de confiança. Você precisará criar um provedor de confiança de identidade de usuário e (opcionalmente) um provedor de confiança baseado em dispositivo, dependendo de suas necessidades.

2. Crie uma instância de acesso verificado, certificando-se de ativar os Padrões Federais de Processo de Informações (FIPS) durante o processo. Além disso, durante a criação, anexe o provedor confiável de Acesso Verificado que você criou na etapa anterior, selecionando-o na lista suspensa.
3. Crie um grupo de Acesso Verificado. Durante a criação do grupo, você o associa à instância de Acesso Verificado recém-criada.
4. Crie um ou mais Endpoints de Acesso Verificado. Durante a criação dos seus endpoints, você os associa ao grupo criado na etapa anterior.

Provedores confiáveis para Acesso Verificado

Um provedor confiável é um serviço que envia informações sobre usuários e dispositivos para Acesso Verificado pela AWS o. Essas informações são chamadas de contexto de confiança. Elas podem incluir atributos baseados na identidade do usuário, como endereço de e-mail ou associação à organização de “vendas”, ou informações sobre os dispositivos, como patches de segurança ou versão do software antivírus.

O Acesso Verificado oferece suporte às seguintes categorias de provedores de confiança:

- Identidade do usuário: um serviço de provedor de identidade (IdP) que armazena e gerencia identidades digitais para usuários.
- Gerenciamento de dispositivos: um sistema de gerenciamento de dispositivos para dispositivos como laptops, tablets e smartphones.

Conteúdo

Provedores de confiança de identidade de usuário para acesso verificado

Você pode optar por usar um AWS IAM Identity Center ou um provedor confiável de identidade de usuário compatível com o OpenID Connect.

Conteúdo

Usando o IAM Identity Center como um provedor confiável

Você pode usar AWS IAM Identity Center como seu provedor confiável de identidade de usuário com o Acesso AWS Verificado.

Pré-requisitos e considerações

- Sua instância do IAM Identity Center deve ser uma AWS Organizations instância. Uma instância autônoma AWS do IAM Identity Center não funcionará.
- Sua instância do IAM Identity Center deve estar habilitada na mesma AWS região em que você deseja criar o provedor confiável de acesso verificado.

Consulte Gerenciar instâncias de organização e conta do IAM Identity Center no Guia AWS IAM Identity Center do usuário para obter detalhes sobre os diferentes tipos de instância.

Crie um provedor confiável do IAM Identity Center

Depois que o IAM Identity Center for ativado em sua AWS conta, você poderá usar o procedimento a seguir para configurar o IAM Identity Center como seu provedor confiável para acesso verificado.

Para criar um provedor confiável do IAM Identity Center (AWS console)

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Provedores de confiança de Acesso Verificado e, em seguida, Criar provedor de confiança de Acesso Verificado.
3. (Opcional) Em Tag de nome e Descrição, insira um nome e uma descrição para o provedor confiável.
4. Em Nome de referência da política, insira um identificador para usar posteriormente ao trabalhar com regras de política.
5. Em Tipo de provedor confiável, selecione Provedor de confiança do usuário.
6. Em Tipo de provedor de confiança do usuário, selecione IAMIdentity Center.
7. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
8. Escolha Criar provedor confiável de Acesso Verificado.

Para criar um provedor confiável do IAM Identity Center (AWS CLI)

- create-verified-access-trust-provedor ()AWS CLI

Excluir um provedor confiável do IAM Identity Center

Antes de excluir um provedor confiável, você deve remover todas as configurações de endpoints e grupos da instância à qual o provedor de confiança está conectado.

Para excluir um provedor confiável do IAM Identity Center (AWS console)

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Provedores de confiança de Acesso Verificado e, em seguida, selecione o provedor de confiança que você deseja excluir em Provedores de confiança de Acesso Verificado.
3. Escolha Ações e, em seguida, Excluir provedor confiável de Acesso Verificado.
4. Confirme a exclusão inserindo `delete` na caixa de texto.
5. Escolha Excluir.

Para excluir um provedor confiável do IAM Identity Center (AWS CLI)

- delete-verified-access-trust-provedor ()AWS CLI

Use um provedor de confiança do OpenID Connect

Acesso Verificado pela AWS oferece suporte a provedores de identidade que usam métodos padrão do OpenID Connect (OIDC). Você pode usar provedores OIDC compatíveis como provedores confiáveis de identidade de usuário com acesso verificado. No entanto, devido à grande variedade de OIDC fornecedores em potencial, não AWS é possível testar cada OIDC integração com o Verified Access.

O Verified Access obtém os dados de confiança que avalia dos do OIDC provedor. `UserInfo Endpoint` O `Scope` parâmetro é usado para determinar quais conjuntos de dados de confiança serão recuperados. Depois que os dados de confiança são recebidos, a política do Acesso Verificado é avaliada em relação a eles.

> **Note**
>
> O Acesso Verificado não usa dados confiáveis `ID token` enviados pelo OIDC provedor ao avaliar a política de Acesso Verificado. Somente os dados de confiança do `UserInfo Endpoint` são avaliados de acordo com a política.

Conteúdo

Pré-requisitos para criar um provedor confiável OIDC

Você precisará coletar as seguintes informações diretamente do serviço do seu provedor de confiança:

- Emissor
- Endpoint de Autorização
- Endpoint de token
- UserInfo ponto final
- ID do cliente
- Segredo do cliente
- Escopo

Crie um provedor de OIDC confiança

Use o procedimento a seguir para criar um OIDC como seu provedor de confiança.

Para criar um provedor de OIDC confiança (AWS console)

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Provedores de confiança de Acesso Verificado e, em seguida, Criar provedor de confiança de Acesso Verificado.
3. (Opcional) Em Tag de nome e Descrição, insira um nome e uma descrição para o provedor confiável.
4. Em Nome de referência da política, insira um identificador para usar posteriormente ao trabalhar com regras de política.
5. Em Tipo de provedor confiável, selecione Provedor de confiança do usuário.
6. Em Tipo de provedor de confiança do usuário, selecione OIDC(OpenID Connect).

7. Em Emissor, insira o identificador do OIDC emissor.
8. Em Ponto final de autorização, insira o ponto final URL de autorização completo.
9. Em Ponto final do token, insira o ponto final completo URL do token.
10. Em Ponto final do usuário, insira o ponto final completo URL do usuário.
11. Insira o identificador do cliente OAuth 2.0 para ID do cliente.
12. Insira o segredo do cliente OAuth 2.0 para Segredo do cliente.
13. Insira uma lista delimitada por espaços dos escopos definidos com seu provedor de identidade. No mínimo, o escopo “openid” é necessário para o Scope.
14. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
15. Escolha Criar provedor confiável de Acesso Verificado.

> **Note**
>
> Você precisará adicionar um redirecionamento URI à lista de permissões do seu OIDC provedor. Você desejará usar o endpoint `ApplicationDomain` de Acesso Verificado para essa finalidade. Isso pode ser encontrado na AWS Management Console guia Detalhes do seu endpoint de acesso verificado ou usando o AWS CLI para descrever o endpoint. Adicione o seguinte à lista de permissões do seu OIDC provedor: https://`ApplicationDomain`/oauth2/idpresponse

Para criar um provedor de OIDC confiança (AWS CLI)

- create-verified-access-trust-provedor ()AWS CLI

Modificar um provedor de OIDC confiança

Depois de criar um provedor confiável, você poderá atualizar a configuração.

Para modificar um provedor de OIDC confiança (AWS console)

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Provedores de confiança de Acesso Verificado e, em seguida, selecione o provedor de confiança que você deseja modificar em Provedores de confiança de Acesso Verificado.

3. Escolha Ações e, em seguida, Modificar provedor confiável de Acesso Verificado.
4. Altere as configurações que deseja modificar.
5. Escolha Modificar provedor confiável de Acesso Verificado.

Para modificar um provedor de OIDC confiança (AWS CLI)

- modify-verified-access-trust-provedor ()AWS CLI

Excluir um provedor de OIDC confiança

Antes de excluir um provedor confiável de usuários, primeiro você precisa remover todas as configurações de endpoints e grupos da instância à qual o provedor de confiança está vinculado.

Para excluir um provedor de OIDC confiança (AWS console)

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Provedores de confiança de Acesso Verificado e, em seguida, selecione o provedor de confiança que você deseja excluir em Provedores de confiança de Acesso Verificado.
3. Escolha Ações e, em seguida, Excluir provedor confiável de Acesso Verificado.
4. Confirme a exclusão inserindo `delete` na caixa de texto.
5. Escolha Excluir.

Para excluir um provedor de OIDC confiança (AWS CLI)

- delete-verified-access-trust-provedor ()AWS CLI

Provedores de confiança baseados em dispositivos para acesso verificado

Você pode usar provedores confiáveis de dispositivos com acesso AWS verificado. Você pode usar um ou vários provedores confiáveis de dispositivos com a instância do Acesso Verificado.

Conteúdo

- Fornecedores confiáveis de dispositivos compatíveis

- Crie um provedor de confiança baseado em dispositivos
- Modificar um provedor de confiança baseado em dispositivo
- Excluir um provedor de confiança baseado em dispositivo

Fornecedores confiáveis de dispositivos compatíveis

Os seguintes provedores confiáveis de dispositivos podem ser integrados ao Acesso Verificado:

- CrowdStrike — Protegendo aplicativos privados com acesso CrowdStrike verificado
- Jamf: integrar o Acesso Verificado com o Jamf Device Identity
- JumpCloud — Acesso integrado JumpCloud e AWS verificado

Crie um provedor de confiança baseado em dispositivos

Siga estas etapas para criar e configurar um provedor confiável de dispositivos para usar com o Acesso Verificado.

Para criar um provedor confiável de dispositivos de acesso verificado (AWS console)

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Provedores de confiança de Acesso Verificado e, em seguida, Criar provedor de confiança de Acesso Verificado.
3. (Opcional) Em Tag de nome e Descrição, insira um nome e uma descrição para o provedor confiável.
4. Insira um identificador para usar posteriormente ao trabalhar com regras de política para o nome de referência da política.
5. Em Tipo de provedor confiável, selecione Identidade do dispositivo.
6. Em Tipo de identidade do dispositivo, escolha Jamf, CrowdStrike, ou JumpCloud.
7. Em ID do inquilino, insira o identificador do aplicativo do inquilino.
8. (Opcional) Em Chave de assinatura pública URL, insira a chave exclusiva URL compartilhada pelo provedor confiável do seu dispositivo. (Esse parâmetro não é necessário para Jamf CrowdStrike ou Jumpcloud.)
9. Escolha Criar provedor confiável de Acesso Verificado.

> **Note**
>
> Você precisará adicionar um redirecionamento URI à lista de permissões do seu OIDC provedor. Você desejará usar o endpoint `DeviceValidationDomain` de Acesso Verificado para essa finalidade. Isso pode ser encontrado na AWS Management Console guia Detalhes do seu endpoint de acesso verificado ou usando o AWS CLI para descrever o endpoint. Adicione o seguinte à lista de permissões do seu OIDC provedor: https://`DeviceValidationDomain`/oauth2/idpresponse

Para criar um provedor confiável de dispositivos de acesso verificado (AWS CLI)

- create-verified-access-trust-provedor ()AWS CLI

Modificar um provedor de confiança baseado em dispositivo

Depois de criar um provedor confiável, você poderá atualizar a configuração.

Para modificar um provedor confiável de dispositivos de acesso verificado (AWS console)

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Fornecedores confiáveis de Acesso Verificado.
3. Selecione o provedor de confiança.
4. Escolha Ações e, em seguida, selecione Modificar provedor confiável de Acesso Verificado.
5. Modifique a descrição conforme necessário.
6. (Opcional) Para Chave de assinatura pública URL, modifique a chave exclusiva URL compartilhada pelo provedor confiável do seu dispositivo. (Esse parâmetro não é necessário se o provedor de confiança do seu dispositivo for Jamf CrowdStrike ou Jumpcloud.)
7. Escolha Modificar provedor confiável de Acesso Verificado.

Para modificar um provedor confiável de dispositivos de acesso verificado (AWS CLI)

- modify-verified-access-trust-provedor ()AWS CLI

Excluir um provedor de confiança baseado em dispositivo

Quando terminar de usar um provedor confiável, você poderá excluí-lo.

Para excluir um provedor confiável de dispositivos de acesso verificado (AWS console)

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Fornecedores confiáveis de Acesso Verificado.
3. Selecione o provedor de confiança que você deseja excluir em Provedores de confiança de Acesso Verificado.
4. Escolha Ações e, em seguida, selecione Excluir provedor confiável de Acesso Verificado.
5. Quando a confirmação for solicitada, insira **`delete`** e escolha Excluir.

Para excluir um provedor confiável de dispositivos de acesso verificado (AWS CLI)

- delete-verified-access-trust-provedor ()AWS CLI

Grupos de Acesso Verificado

Um Acesso Verificado pela AWS grupo é uma coleção de endpoints de acesso verificado e uma política de acesso verificado em nível de grupo. Cada endpoint dentro de um grupo compartilha a política do Acesso Verificado. Você pode usar grupos para reunir endpoints que tenham requisitos de segurança comuns. Isso pode ajudar a simplificar a administração de políticas usando uma política para as necessidades de segurança de vários aplicativos.

Por exemplo, você pode agrupar todos os aplicativos de vendas e definir uma política de acesso para todo o grupo. Em seguida, você pode usar essa política para definir um conjunto comum de requisitos mínimos de segurança para todos os aplicativos de vendas. Essa abordagem ajuda a simplificar a administração de políticas.

Quando você cria um grupo, é necessário associar o grupo a uma instância do Acesso Verificado. Durante o processo de criação de um endpoint, você associará o endpoint a um grupo.

Tarefas

- Criar um grupo do Acesso Verificado
- Modificar uma política de grupo do Acesso Verificado
- Excluir um grupo do Acesso Verificado

Criar um grupo do Acesso Verificado

Siga o procedimento abaixo para criar um novo grupo de Acesso Verificado.

Para criar um grupo do Acesso Verificado

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Grupos de Acesso Verificado e, em seguida, Criar grupo de Acesso Verificado.
3. (Opcional) Em Tag de nome e Descrição, insira um nome e uma descrição para o grupo.
4. Para Instância de Acesso Verificado, selecione uma instância de Acesso Verificado para associar ao grupo.
5. (Opcional) Para definição de política, insira uma política de acesso do Acesso Verificado a ser aplicada ao grupo.

6. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
7. Escolha Criar grupo de Acesso Verificado.

Modificar uma política de grupo do Acesso Verificado

Use o procedimento a seguir para modificar uma política de grupo do Acesso Verificado.

Para modificar uma política de grupo do Acesso Verificado

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha grupos do Acesso Verificado e, em seguida, selecione o grupo cuja política você deseja modificar.
3. Escolha Ações e, em seguida, Modificar política de grupo de Acesso Verificado.
4. (Opcional) Ative ou desative a opção Ativar política, dependendo da sua meta atual.
5. (Opcional) Em Política, insira uma política do Acesso Verificado a ser aplicada ao grupo.
6. Escolha Modificar política de grupo de Acesso Verificado.

Excluir um grupo do Acesso Verificado

Quando não precisar mais de um grupo de Acesso Verificado, você poderá excluir.

Para excluir um grupo do Acesso Verificado

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha grupos de Acesso Verificado.
3. Selecione o grupo do.
4. Escolha Ações, Excluir grupo de Acesso Verificado.
5. Quando a confirmação for solicitada, insira **`delete`** e escolha Excluir.

Endpoints de Acesso Verificado

Um endpoint de Acesso Verificado representa um aplicativo. Cada endpoint está associado a um grupo de Acesso Verificado e herda a política de acesso do grupo. Opcionalmente, você pode anexar uma política de endpoint específica do aplicativo a cada endpoint.

Conteúdo

Tipos de endpoint de Acesso Verificado

A seguir estão os possíveis tipos de endpoint de acesso verificado:

- Balanceador de carga: as solicitações do aplicativo são enviadas a um balanceador de carga para distribuí-las ao seu aplicativo.
- Interface de rede: as solicitações do aplicativo são enviadas para uma interface de rede usando o protocolo e a porta especificados.

Como o Acesso Verificado funciona com redes compartilhadas VPCs e sub-redes

A seguir estão os comportamentos em relação às VPC sub-redes compartilhadas:

- Os endpoints de acesso verificado são compatíveis com o compartilhamento de VPC sub-rede. Um participante pode criar um endpoint de Acesso Verificado em uma sub-rede compartilhada.
- O participante que criou o endpoint será o proprietário do endpoint e a única pessoa autorizada a modificá-lo. O VPC proprietário não poderá modificar o endpoint.

- Os endpoints de acesso verificado não podem ser criados em uma Zona AWS Local e, portanto, o compartilhamento por meio de Zonas Locais não é possível.

Para obter mais informações, consulte Compartilhe sua VPC com outras contas no Guia do VPC usuário da Amazon.

Crie um endpoint de balanceador de carga para Acesso Verificado

Use o procedimento a seguir para criar um endpoint de balanceador de carga para acesso verificado. Para mais informações sobre balanceador de carga consulte o Manual do usuário do balanceador de carga elástico.

Requisitos

- Somente IPv4 o tráfego é suportado.
- Somente os HTTPS protocolos HTTP e são suportados.
- O balanceador de carga precisa ser um Application Load Balancer ou um Network Load Balancer, e precisa ser um balanceador de carga interno.
- O balanceador de carga e as sub-redes devem pertencer à mesma nuvem privada virtual (). VPC
- HTTPSos balanceadores de carga podem usar certificados autoassinados ou públicosTLS.
- Você deve fornecer um nome de domínio para seu aplicativo. Esse é o DNS nome público que seus usuários usarão para acessar seu aplicativo. Você também precisará fornecer um SSL certificado público com um CN que corresponda a esse nome de domínio. Você pode criar ou importar o certificado usando AWS Certificate Manager.

Para criar um endpoint do balanceador de carga

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints de Acesso Verificado.
3. Escolha Criar endpoint de Acesso Verificado.
4. (Opcional) Em Tag de nome e Descrição, insira um nome e uma descrição para o endpoint.
5. Para o grupo de Acesso Verificado, escolha um grupo de Acesso Verificado para o endpoint.
6. Para obter detalhes do aplicativo faça o seguinte:

    a. Em Domínio do aplicativo, insira um DNS nome para seu aplicativo.

b. Em Certificado de domínio ARN, escolha o TLS certificado público.

7. Em Detalhes do endpoint, faça o seguinte:

   a. Em Tipo de anexo, escolha VPC.

   b. Em Grupos de segurança selecione o grupos de segurança para o endpoint. O tráfego do endpoint de Acesso Verificado que entra no seu balanceador de carga será associado a esse grupo de segurança.

   c. Em Prefixo de domínio do Endpoint, insira um identificador personalizado para acrescentar ao DNS nome que o Verified Access gera para o endpoint.

   d. Em Tipo de endpoint escolha balanceador de carga.

   e. Para Protocolo, escolha HTTPSou HTTP.

   f. Sob Porta, digite o número da porta.

   g. Em Balanceador de carga ARN, escolha o balanceador de carga.

   h. Em Sub-redes, escolha as sub-redes do seu balanceador de carga.

8. (Opcional) Para definição de política, insira uma política do Acesso Verificado para o endpoint.
9. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
10. Escolha Criar endpoint de Acesso Verificado.

Criar um endpoint da interface de rede para Acesso Verificado

Use o seguinte procedimento para criar um endpoint de interface de rede.

Requisitos

- Somente IPv4 o tráfego é suportado.
- Somente os HTTPS protocolos HTTP e são suportados.
- A interface de rede deve pertencer à mesma nuvem privada virtual (VPC) dos grupos de segurança.
- Usamos o IP privado na interface de rede para encaminhar o tráfego.
- Você deve fornecer um nome de domínio para seu aplicativo. Esse é o DNS nome público que seus usuários usarão para acessar seu aplicativo. Você também precisará fornecer um SSL certificado público com um CN que corresponda a esse nome de domínio. Você pode criar ou importar o certificado usando AWS Certificate Manager.

Para criar um endpoint de interface de rede

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints de Acesso Verificado.
3. Escolha Criar endpoint de Acesso Verificado.
4. (Opcional) Em Tag de nome e Descrição, insira um nome e uma descrição para o endpoint.
5. Para o grupo de Acesso Verificado, escolha um grupo de Acesso Verificado para o endpoint.
6. Para obter detalhes do aplicativo faça o seguinte:
   a. Em Domínio do aplicativo, insira o DNS nome do seu aplicativo.
   b. Em Certificado de domínio ARN, escolha o TLS certificado público.
7. Em Detalhes do endpoint, faça o seguinte:
   a. Em Tipo de anexo, escolha VPC.
   b. Em Grupos de segurança selecione o grupos de segurança para o endpoint. O tráfego do endpoint de Acesso Verificado que entra na interface de rede será associado a esse grupo de segurança.
   c. Em Prefixo de domínio do Endpoint, insira um identificador personalizado para acrescentar ao DNS nome que o Verified Access gera para o endpoint.
   d. Em Tipo de endpoint, selecione Interface de rede.
   e. Para Protocolo, escolha HTTPSou HTTP.
   f. Sob Porta, digite o número da porta.
   g. Em Interface de rede, escolha a interface de rede.
8. (Opcional) Para definição de política, insira uma política do Acesso Verificado para o endpoint.
9. (Opcional) Para adicionar uma tag, escolha Adicionar nova tag e insira a chave e o valor da tag.
10. Escolha Criar endpoint de Acesso Verificado.

Permita o tráfego originado do seu endpoint de Acesso Verificado

Você pode configurar os grupos de segurança de seus aplicativos para que eles permitam o tráfego originado do seu endpoint de Acesso Verificado. Você faz isso adicionando uma regra de entrada que especifica o grupo de segurança do endpoint como a origem. Recomendamos que você remova todas as regras de entrada adicionais, para que seu aplicativo receba tráfego somente do seu endpoint de Acesso Verificado.

Recomendamos que você mantenha as regras de saída existentes.

Para atualizar as regras do grupo de segurança do seu aplicativo

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints de Acesso Verificado.
3. Escolha o endpoint de acesso verificado, localize o grupo Segurança IDs na guia Detalhes e copie a ID do grupo de segurança do seu endpoint.
4. No painel de navegação, selecione Grupos de segurança.
5. Marque a caixa de seleção do grupo de segurança associado ao seu alvo e escolha Ações, Editar regras de entrada.
6. Para adicionar uma regra de grupo de segurança que permita o tráfego originado do seu endpoint de Acesso Verificado, faça o seguinte:
   a. Escolha Adicionar regra.
   b. Em Tipo, escolha Todo o tráfego, ou um tipo específico de tráfego que você deseja permitir.
   c. Para Origem, escolha Personalizada e digite o ID do grupo de segurança de seu endpoint.
7. (Opcional) Para exigir que o tráfego seja originado somente do seu endpoint de Acesso Verificado, exclua todas as outras regras do grupo de segurança de entrada.
8. Escolha Salvar regras.

Modificar um endpoint do Acesso Verificado

Depois de criar um endpoint de acesso verificado, você pode modificar sua configuração.

Para modificar um endpoint do Acesso Verificado

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints de Acesso Verificado.
3. Selecione o endpoint.
4. Escolha Ações, Modificar endpoint de Acesso Verificado.
5. Modifique os detalhes do endpoint conforme necessário.
6. Escolha Modificar endpoint de Acesso Verificado.

Modificar uma política de endpoint do Acesso Verificado

Após criar um endpoint do Acesso Verificado, é possível modificar a política.

Para modificar uma política de endpoint do Acesso Verificado

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints de Acesso Verificado.
3. Selecione o endpoint cuja política você queira modificar.
4. Escolha Ações, Modificar política de endpoint de Acesso Verificado.
5. (Opcional) Ative ou desative a opção Ativar política, dependendo da sua meta atual.
6. (Opcional) Em Política, insira uma política do Acesso Verificado a ser aplicada ao endpoint.
7. Escolha Modificar política de endpoint de Acesso Verificado.

Excluir um endpoint do Acesso Verificado

Quando não precisar mais de um endpoint do Acesso Verificado, você poderá excluí-lo.

Para excluir um endpoint do Acesso Verificado

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints de Acesso Verificado.
3. Selecione o endpoint.
4. Escolha Ações, Excluir endpoint de Acesso Verificado.
5. Quando a confirmação for solicitada, insira **`delete`** e escolha Excluir.

Dados de confiança enviados ao Verified Access por provedores confiáveis

Dados confiáveis são dados Acesso Verificado pela AWS enviados por um provedor confiável. Os dados de confiança também são chamados de “declarações do usuário” ou “contexto de confiança”. Os dados geralmente incluem informações sobre um usuário ou um dispositivo. Exemplos de dados de confiança incluem e-mail do usuário, associação ao grupo, versão do sistema operacional do dispositivo, estado de segurança do dispositivo e assim por diante. As informações enviadas variam de acordo com o provedor de confiança, então você deve consultar a documentação do seu provedor de confiança para obter uma lista completa e atualizada dos dados de confiança.

No entanto, usando os recursos de logs de Acesso Verificado, você também pode ver quais dados de confiança estão sendo enviados pelo seu provedor de confiança. Isso pode ser útil ao definir políticas que permitem ou negam acesso aos seus aplicativos. Para obter informações sobre como incluir contexto de confiança em seus logs, consulte Ativar ou desativar o contexto de confiança do Acesso Verificado.

Esta seção contém exemplos de dados de confiança e exemplos para ajudar você a começar a escrever políticas. As informações fornecidas aqui são apenas para fins ilustrativos e não como referência oficial.

Conteúdo

Contexto padrão para dados de confiança do Verified Access

Acesso Verificado pela AWS inclui alguns elementos sobre a HTTP solicitação atual por padrão em todas as avaliações do Cedar, independentemente dos provedores de confiança configurados. Quando uma política é avaliada, o Acesso Verificado inclui dados sobre a HTTP solicitação atual no contexto do Cedar sob o. `context.http_request key` Você pode escrever uma política que avalie os dados, se quiser. O JSONesquema a seguir mostra quais dados estão incluídos na avaliação.

```
{
     "title": "HTTP Request data included by Verified Access",
     "type": "object",
     "properties": {
         "user_agent": {
             "type": "string",
             "description": "The value of the User-Agent request header"
         },
         "x_forwarded_for": {
             "type": "string",
             "description": "The value of the X-Forwarded-For request header"
         },
         "http_method": {
             "type": "string",
             "description": "The HTTP Method provided (e.g. GET or POST)"
         },
         "hostname": {
             "type": "string",
             "description": "The value of the Host request header"
         },
         "port": {
            "type": "integer",
            "description": "The value of the verified access endpoint port"
         },
         "client_ip": {
             "type": "string",
             "description": "User ip connecting to the verified access endpoint"
         }
     }
 }
```

Veja a seguir um exemplo de uma política que avalia os dados da HTTP solicitação.

```
forbid(principal, action, resource) when {
   context.http_request.http_method == "POST"
   && !(context.identity.roles.contains("Administrator"))
 };
```

AWS IAM Identity Center contexto para dados de confiança do Verified Access

Quando uma política é avaliada, se você definir AWS IAM Identity Center como um provedor de confiança, Acesso Verificado pela AWS inclua os dados de confiança no contexto do Cedar sob a chave que você especifica como “Nome de referência da política” na configuração do provedor de confiança. Você pode escrever uma política que avalie os dados de confiança, se quiser.

> **Note**
>
> A chave de contexto do seu provedor de confiança vem do nome de referência da política que você configura ao criar o provedor de confiança. Por exemplo, se você configurar o nome de referência da política como “idp123”, a chave de contexto será “context.idp123”. Verifique se está usando a chave de contexto correta ao criar a política.

O JSONesquema a seguir mostra quais dados estão incluídos na avaliação.

```
{
   "title": "AWS IAM Identity Center context specification",
   "type": "object",
   "properties": {
     "user": {
       "type": "object",
       "properties": {
         "user_id": {
           "type": "string",
           "description": "a unique user id generated by AWS IdC"
         },
         "user_name": {
           "type": "string",
           "description": "username provided in the directory"
         },
         "email": {
           "type": "object",
           "properties": {
             "address": {
               "type": "email",
               "description": "email address associated with the user"
             },
```

```
              "verified": {
                "type": "boolean",
                "description": "whether the email address has been verified by AWS IdC"
              }
            }
          }
        }
      },
      "groups": {
        "type": "object",
        "description": "A list of groups the user is a member of",
        "patternProperties": {
          "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{12}$": {
            "type": "object",
            "description": "The Group ID of the group",
            "properties": {
              "group_name": {
                "type": "string",
                "description": "The customer-provided name of the group"
              }
            }
          }
        }
      }
    }
  }
```

Veja a seguir um exemplo de uma política que avalia os dados de confiança fornecidos pela AWS IAM Identity Center.

```
permit(principal, action, resource) when {
   context.idc.user.email.verified == true
   // User is in the "sales" group with specific ID
   && context.idc.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
 };
```

> **Note**
>
> Como os nomes dos grupos podem ser alterados, o IAM Identity Center se refere aos grupos usando seu ID de grupo. Isso ajuda a evitar a violação de uma declaração de política ao alterar o nome de um grupo.

Contexto de provedor de confiança de terceiros para dados de confiança do Verified Access

Esta seção descreve os dados de confiança fornecidos Acesso Verificado pela AWS por provedores de confiança terceirizados.

> **Note**
>
> A chave de contexto do seu provedor de confiança vem do nome de referência da política que você configura ao criar o provedor de confiança. Por exemplo, se você configurar o nome de referência da política como “idp123”, a chave de contexto será “context.idp123”. Confira se está usando a chave de contexto correta ao criar a política.

Conteúdo

Extensão do navegador

Se você planeja incorporar o contexto de confiança do dispositivo em suas políticas de acesso, precisará da extensão de navegador de Acesso AWS Verificado ou da extensão de navegador de outro parceiro. Atualmente, o Acesso Verificado é compatível com os navegadores Google Chrome e Mozilla Firefox.

Atualmente, oferecemos suporte a três provedores confiáveis de dispositivos: Jamf (que oferece suporte a dispositivos macOS) CrowdStrike , (que oferece suporte a dispositivos Windows 11 e Windows 10) JumpCloud e (que oferece suporte a Windows e macOS).

- Se você estiver usando dados de confiança do Jamf em suas políticas, seus usuários deverão baixar e instalar a extensão do Acesso Verificado pela AWS navegador da loja virtual do Chrome ou do site de complementos do Firefox em seus dispositivos.
- Se você estiver usando dados CrowdStrikeconfiáveis em suas políticas, primeiro seus usuários precisarão instalar o Acesso Verificado pela AWS Native Messaging Host (link direto para download). Esse componente é necessário para obter os dados de confiança do CrowdStrike agente em execução nos dispositivos dos usuários. Depois de instalar esse componente, os usuários devem instalar a extensão do Acesso Verificado pela AWS navegador da loja virtual do Chrome ou do site de complementos do Firefox em seus dispositivos.
- Se você estiver usando JumpCloud, seus usuários devem ter a extensão de JumpCloud navegador da loja virtual do Chrome ou do site de complementos do Firefox instalada em seus dispositivos.

Jamf

Jamf é um provedor de confiança de terceiros. Quando uma política é avaliada, se você definir o Jamf como um provedor confiável, o Acesso Verificado incluirá os dados de confiança no contexto do Cedar sob a chave especificada como “Nome de referência da política” na configuração do provedor de confiança. Você pode escrever uma política que avalie os dados de confiança, se quiser. O JSONesquema a seguir mostra quais dados estão incluídos na avaliação.

Para obter mais informações sobre como usar o Jamf com acesso verificado, consulte Integração do acesso AWS verificado com o Jamf Device Identity no site do Jamf.

```
{
    "title": "Jamf device data specification",
    "type": "object",
    "properties": {
        "iss": {
            "type": "string",
            "description": "\"Issuer\" - the Jamf customer ID"
        },
        "iat": {
            "type": "integer",
```

```
            "description": "\"Issued at Time\" - a unixtime (seconds since epoch) value
 of when the device information data was generated"
        },
        "exp": {
            "type": "integer",
            "description": "\"Expiration\" - a unixtime (seconds since epoch) value for
 when this device information is no longer valid"
        },
        "sub": {
            "type": "string",
            "description": "\"Subject\" - either the hardware UID or a value generated
 based on device location"
        },
        "groups": {
            "type": "array",
            "description": "Group IDs from UEM connector sync",
            "items": {
                "type": "string"
            }
        },
        "risk": {
            "type": "string",
            "enum": [
                "HIGH",
                "MEDIUM",
                "LOW",
                "SECURE",
                "NOT_APPLICABLE"
            ],
            "description": "a Jamf-reported level of risk associated with the device."
        },
        "osv": {
            "type": "string",
            "description": "The version of the OS that is currently running, in Apple
 version number format (https://support.apple.com/en-us/HT201260)"
        }
    }
}
```

Veja a seguir um exemplo de política que avalia os dados de confiança fornecidos pelo Jamf.

```
permit(principal, action, resource) when {
   context.jamf.risk == "LOW"
```

```
};
```

O Cedar fornece uma `.contains()` função útil para ajudar com enumerações, como a pontuação de risco de Jamf.

```
permit(principal, action, resource) when {
   ["LOW", "SECURE"].contains(context.jamf.risk)
};
```

CrowdStrike

CrowdStrike é um provedor fiduciário terceirizado. Quando uma política é avaliada, se você definir CrowdStrike como um provedor de confiança, o Acesso Verificado inclui os dados de confiança no contexto do Cedar sob a chave que você especifica como “Nome de referência da política” na configuração do provedor de confiança. Você pode escrever uma política que avalie os dados de confiança, se quiser. O JSONesquema a seguir mostra quais dados estão incluídos na avaliação.

Para obter mais informações sobre como usar CrowdStrike com o Acesso Verificado, consulte Protegendo aplicativos privados com CrowdStrike e Acesso Verificado pela AWS no GitHub site.

```
{
  "title": "CrowdStrike device data specification",
  "type": "object",
  "properties": {
    "assessment": {
      "type": "object",
      "description": "Data about CrowdStrike's assessment of the device",
      "properties": {
        "overall": {
          "type": "integer",
          "description": "A single metric, between 1-100, that accounts as a weighted
 average of the OS and and Sensor Config scores"
        },
        "os": {
          "type": "integer",
          "description": "A single metric, between 1-100, that accounts for the OS-
specific settings monitored on the host"
        },
        "sensor_config": {
          "type": "integer",
          "description": "A single metric, between 1-100, that accounts for the
 different sensor policies monitored on the host"
```

```
        },
        "version": {
          "type": "string",
          "description": "The version of the scoring algorithm being used"
        }
      }
    },
    "cid": {
      "type": "string",
      "description": "Customer ID (CID) unique to the customer's environemnt"
    },
    "exp": {
      "type": "integer",
      "description": "unixtime, The expiration time of the token"
    },
    "iat": {
      "type": "integer",
      "description": "unixtime, The issued time of the token"
    },
    "jwk_url": {
      "type": "string",
      "description": "URL that details the JWT signing"
    },
    "platform": {
      "type": "string",
      "enum": ["Windows 10", "Windows 11", "macOS"],
      "description": "Operating system of the endpoint"
    },
    "serial_number": {
      "type": "string",
      "description": "The serial number of the device derived by unique system
information"
    },
    "sub": {
      "type": "string",
      "description": "Unique CrowdStrike Agent ID (AID) of machine"
    },
    "typ": {
      "type": "string",
      "enum": ["crowdstrike-zta+jwt"],
      "description": "Generic name for this JWT media. Client MUST reject any other
type"
    }
  }
```

```
}
```

Veja a seguir um exemplo de uma política que avalia os dados de confiança fornecidos pela CrowdStrike.

```
permit(principal, action, resource) when {
   context.crowdstrike.assessment.overall > 50
};
```

JumpCloud

JumpCloud é um provedor fiduciário terceirizado. Quando uma política é avaliada, se você definir JumpCloud como um provedor de confiança, o Acesso Verificado inclui os dados de confiança no contexto do Cedar sob a chave que você especifica como “Nome de referência da política” na configuração do provedor de confiança. Você pode escrever uma política que avalie os dados de confiança, se quiser. O JSONesquema a seguir mostra quais dados estão incluídos na avaliação.

Para obter mais informações sobre como usar JumpCloud com o Acesso AWS Verificado, consulte Integração JumpCloud e Acesso AWS Verificado no JumpCloud site.

```
{
  "title": "JumpCloud device data specification",
  "type": "object",
  "properties": {
    "device": {
      "type": "object",
      "description": "Properties of the device",
      "properties": {
        "is_managed": {
          "type": "boolean",
          "description": "Boolean to indicate if the device is under management"
        }
      }
    },
    "exp": {
      "type": "integer",
      "description": "Expiration. Unixtime of the token's expiration."
    },
    "durt_id": {
      "type": "string",
      "description": "Device User Refresh Token ID. Unique ID that represents the
 device + user."
```

```
    },
    "iat": {
      "type": "integer",
      "description": "Issued At. Unixtime of the token's issuance."
    },
    "iss": {
      "type": "string",
      "description": "Issuer. This will be 'go.jumpcloud.com'"
    },
    "org_id": {
      "type": "string",
      "description": "The JumpCloud Organization ID"
    },
    "sub": {
      "type": "string",
      "description": "Subject. The managed JumpCloud user ID on the device."
    },
    "system": {
      "type": "string",
      "description": "The JumpCloud system ID"
    }
  }
}
```

Veja a seguir um exemplo de uma política que avalia o contexto de confiança fornecido pela JumpCloud.

```
permit(principal, action, resource) when {
   context.jumpcloud.org_id = 'Unique_orgnaization_identifier'
};
```

O usuário reivindica aprovação e verificação de assinatura no Acesso Verificado

Depois que uma Acesso Verificado pela AWS instância autentica um usuário com sucesso, ela envia as declarações de usuário recebidas do IdP para o endpoint de acesso verificado. As declarações do usuário são assinadas para que os aplicativos possam verificar as assinaturas e também verificar se as solicitações foram enviadas pelo Acesso Verificado. Durante esse processo, o seguinte HTTP cabeçalho é adicionado:

`x-amzn-ava-user-context`

Esse cabeçalho contém as declarações do usuário no formato JSON web token (JWT). O JWT formato inclui um cabeçalho, carga útil e assinatura codificados em base64URL. O Verified Access usa ES384 (algoritmo de ECDSA assinatura usando o algoritmo de hash SHA -384) para gerar a assinatura. JWT

Os aplicativos podem usar essas declarações para personalização ou outras experiências específicas do usuário. Os desenvolvedores de aplicativos devem se informar sobre o nível de exclusividade e verificação de cada declaração fornecida pelo provedor de identidade antes do uso. A reivindicação `sub` é a melhor maneira de identificar determinado usuário.

Conteúdo

Exemplo: Assinado JWT para reivindicações de OIDC usuários

Os exemplos a seguir demonstram a aparência do cabeçalho e da carga útil das declarações do OIDC usuário no JWT formato.

Exemplo de cabeçalho:

```
{
"alg": "ES384",
"kid": "12345678-1234-1234-1234-123456789012",
"signer": "arn:aws:ec2:us-east-1:123456789012:verified-access-instance/vai-
abc123xzy321a2b3c",
"iss": "OIDC Issuer URL"
"exp": "expiration" (120 secs)
}
```

Exemplo de carga:

```
{
"sub": "xyzsubject",
"email": "xxx@amazon.com",
"email_verified": true,
"groups": [
```

```
"Engineering",
"finance"
]
}
```

Exemplo: Assinado JWT para reivindicações de usuários do IAM Identity Center

Os exemplos a seguir demonstram a aparência do cabeçalho e da carga útil das declarações de usuários do IAM Identity Center no JWT formato.

> **Note**
>
> Para o IAM Identity Center, somente as informações do usuário serão incluídas nas reivindicações.

Exemplo de cabeçalho:

```
{
"alg": "ES384",
"kid": "12345678-1234-1234-1234-123456789012",
"signer": "arn:aws:ec2:us-east-1:123456789012:verified-access-instance/vai-
abc123xzy321a2b3c",
"iss": "arn:aws:ec2:us-east-1:123456789012:verified-access-trust-provider/vatp-
abc123xzy321a2b3c",
"exp": "expiration" (120 secs)
}
```

Exemplo de carga:

```
{
"user": {
        "user_id": "f478d4c8-a001-7064-6ea6-12423523",
        "user_name": "test-123",
        "email": {
            "address": "test@amazon.com",
            "verified": false
        }
    }
```

```
}
```

Chaves públicas

Como as instâncias de acesso verificado não criptografam declarações de usuários, recomendamos que você configure os endpoints de acesso verificado para uso. HTTPS Se você configurar seu endpoint de acesso verificado para usoHTTP, certifique-se de restringir o tráfego para o endpoint usando grupos de segurança.

É recomendável verificar a assinatura antes de fazer qualquer autorização com base nas solicitações. Para obter a chave pública, obtenha o ID da chave do JWT cabeçalho e use-o para pesquisar a chave pública no endpoint. O endpoint para cada um Região da AWS é o seguinte:

`https://public-keys.prod.verified-access.<region>.amazonaws.com/<key-id>`

Exemplo: Recuperação e decodificação JWT

O exemplo de código a seguir mostra como obter o ID de chave, a chave pública e a carga útil em Python 3.9.

```
import jwt
import requests
import base64
import json

# Step 1: Get the key id from JWT headers (the kid field)
encoded_jwt = headers.dict['x-amzn-ava-user-context']
jwt_headers = encoded_jwt.split('.')[0]
decoded_jwt_headers = base64.b64decode(jwt_headers)
decoded_jwt_headers = decoded_jwt_headers.decode("utf-8")
decoded_json = json.loads(decoded_jwt_headers)
kid = decoded_json['kid']

# Step 2: Get the public key from Regional endpoint
url = 'https://public-keys.prod.verified-access.' + region + '.amazonaws.com/' + kid
req = requests.get(url)
pub_key = req.text

# Step 3: Get the payload
payload = jwt.decode(encoded_jwt, pub_key, algorithms=['ES384'])
```

Políticas do Acesso Verificado

Acesso Verificado pela AWS as políticas permitem que você defina regras para acessar seus aplicativos hospedados em AWS. Eles são escritos em cedro, uma linguagem AWS política. Usando o Cedar, você pode criar políticas que são avaliadas em relação aos dados de confiança enviados pelos provedores de confiança baseados em identidade ou dispositivos que você configura para usar com o Acesso Verificado.

Para obter informações mais detalhadas sobre a linguagem política do Cedar, consulte o Guia de referência do Cedar.

Esta seção descreve como as políticas do Acesso Verificado são estruturadas, o que elas contêm, como defini-las e fornece alguns exemplos.

Índice

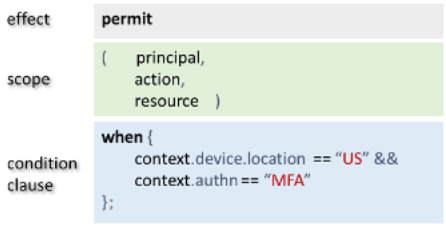
Trabalhe com políticas para o Acesso Verificado

Ao criar um grupo de Acesso Verificado ou criar um endpoint de Acesso Verificado, você tem a opção de definir a política do Acesso Verificado. Você pode criar um grupo ou endpoint sem definir a política do Acesso Verificado, mas todas as solicitações de acesso serão bloqueadas até que você defina uma política.

Para adicionar ou alterar uma política em um grupo ou endpoint de Acesso Verificado existente após sua criação, consulte Modificar uma política de grupo do Acesso Verificado ou Modificar uma política de endpoint do Acesso Verificado.

Estrutura da declaração de política de acesso verificada

Esta seção descreve a declaração Acesso Verificado pela AWS de política e como ela é avaliada. Você pode ter várias declarações em uma única política do Acesso Verificado. O diagrama a seguir mostra uma estrutura de uma política do Acesso Verificado.



A política contém os elementos a seguir:

- Efeito — Especifica se a declaração de política é `permit` (`Allow`) ou `forbid` (`Deny`).
- Escopo: especifica os princípios, as ações e os recursos aos quais o efeito se aplica. Você pode deixar o escopo no Cedar indefinido ao não identificar princípios, ações ou recursos específicos (conforme mostrado no exemplo anterior). Nesse caso, a política se aplica a todos os principais, ações e recursos possíveis.
- Cláusula de condição: especifica o contexto no qual o efeito se aplica.

> **Important**
>
> Para Acesso Verificado, as políticas são totalmente expressas referindo-se aos dados de confiança na cláusula condicional. O escopo da política deve sempre ser mantido indefinido. Em seguida, você pode especificar o acesso usando o contexto de confiança da identidade e do dispositivo na cláusula condicional.

Exemplo simples de política

```
permit(principal,action,resource)
when{
 context.<policy-reference-name>.<attribute> &&
 context.<policy-reference-name>.<attribute2>
};
```

No exemplo anterior, observe que você pode usar mais de uma cláusula de condição em uma declaração de política usando o && operador. A linguagem de políticas do Cedar oferece um poder expressivo para criar declarações de políticas personalizadas, refinadas e abrangentes. Para obter exemplos adicionais, consulte Exemplos de políticas de acesso verificado.

Avaliação da política de acesso verificada

Um documento de política é um conjunto de uma ou mais declarações de política (declarações `permit` ou `forbid`). A política se aplicará se a cláusula condicional (a declaração `when`) for verdadeira. Para que um documento de política permita o acesso, pelo menos uma política de permissão no documento deve ser aplicada e nenhuma política de proibição pode ser aplicada. Se nenhuma política de permissão se aplicar e/ou uma ou mais políticas de proibição se aplicarem, o documento de política negará o acesso. Se você definiu documentos de política para o grupo de acesso verificado e o endpoint de acesso verificado, ambos os documentos devem permitir o acesso. Se você não definiu um documento de política para o endpoint de acesso verificado, somente a política de grupo de acesso verificado precisará permitir o acesso.

> **Note**
>
> Acesso Verificado pela AWS valida a sintaxe ao criar a política, mas não valida os dados inseridos na cláusula condicional.

Operadores integrados para políticas de acesso verificado

Ao criar o contexto de uma Acesso Verificado pela AWS política usando várias condições, conforme discutido emEstrutura da declaração de política de acesso verificada, você pode usar o && operador para adicionar outras condições. Há também muitos outros operadores integrados que você pode usar para adicionar mais poder expressivo às condições da sua política. A tabela a seguir contém todos os operadores integrados para referência.

Operador	Tipos e sobrecargas	Descrição
!	Booleano → Booleano	Lógico que não.
==	qualquer → qualquer	Igualdade. Funciona com argumentos de qualquer tipo,

Operador	Tipos e sobrecargas	Descrição
		mesmo que os tipos não correspondam. Valores de tipos diferentes nunca são iguais entre si.
!=	qualquer → qualquer	Desigualdade; o inverso exato da igualdade (veja acima).
<	(longo, longo) → Booleano	Número inteiro longo menor que.
<=	(longo, longo) → Booleano	Inteiro longo less-than-or-equal -to.
>	(longo, longo) → Booleano	Número inteiro longo maior que.
>=	(longo, longo) → Booleano	Inteiro longo greater-than-or-equal -to.
em	(entidade, entidade) → Booleano	Associação hierárquica (reflexiva: A em A é sempre verdadeiro).
	(entidade, conjunto (entidade)) → Booleano	Associação à hierarquia: A em [B, C,...] é verdadeiro se (A e B) || (A em C) ||... erro se o conjunto não contiver uma entidade.
&&	(Booleano, Booleano) → Booleano	Lógico e (curto-circuito).
||	(Booleano, Booleano) → Booleano	Lógico ou (curto-circuito).
.exists()	entidade→ Booleano	Existência de entidades.

Operador	Tipos e sobrecargas	Descrição
tem	(entidade, atributo) → Booleano	Operador infixo. `e has f` testa se o registro ou a entidade `e` tem uma associação para o atributo `f`. Retorna `false` se `e` não existe ou se `e` existe, mas não tem o atributo `f`. Os atributos podem ser expressos como identificadores ou literais de sequência de caracteres.
como	(string, string) → Booleano	Operador infixo. `t like p` verifica se o texto `t` corresponde ao padrão `p`, que pode incluir caracteres curinga `*` que correspondam a 0 ou mais de qualquer caractere. Para combinar literalmente um caractere estrela `t`, você pode usar a sequência `\*` especial de caracteres escapados em `p`.
.contém()	(conjunto, todos) → Booleano	Defina a associação (B é um elemento de A).
.containsAll()	(conjunto, conjunto) → Booleano	Testa se o conjunto A contém todos os elementos do conjunto B.
.containsAny()	(conjunto, conjunto) → Booleano	Testa se o conjunto A contém algum dos elementos do conjunto B.

Comentários sobre a política de acesso verificado

Você pode incluir declarações de comentários em suas Acesso Verificado pela AWS políticas. Os comentários são definidos como uma linha que começa `//` e termina com uma nova linha.

O exemplo a seguir mostra a instrução correspondente na política.

```
// this policy grants access to users in a given domain with trusted devices
permit(principal, action, resource)
when {
  // the user's email address is in the @example.com domain
  context.idc.user.email.address.contains("@example.com")
  // Jamf thinks the user's computer is low risk or secure.
  && ["LOW", "SECURE"].contains(context.jamf.risk)
};
```

Curto-circuito da lógica da política de acesso verificada

Talvez você queira escrever uma Acesso Verificado pela AWS política que avalie dados que podem ou não estar presentes em um determinado contexto. Se você referenciar dados em um contexto que não existe, o Cedar produzirá um erro e avaliará a política para negar o acesso, independentemente da sua intenção. Por exemplo, isso resultaria em uma negação, pois `fake_provider` e `bogus_key` não existem nesse contexto.

```
permit(principal, action, resource) when {
  context.fake_provider.bogus_key > 42
};
```

Para evitar essa situação, você pode verificar se uma chave está presente usando o `has` operador. Se o operador `has` retornar falso, a avaliação adicional da declaração encadeada será interrompida e o Cedar não produzirá um erro ao tentar referenciar um item que não existe.

```
permit(principal, action, resource) when {
  context.identity.user has "some_key" && context.identity.user.some_key > 42
};
```

Isso é mais útil ao especificar uma política que faz referência a dois provedores de confiança diferentes.

```
permit(principal, action, resource) when {
  // user is in an allowed group
  context.aws_idc.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
  &&(
    (
      // if CrowdStrike data is present,
      // permit if CrowdStrike's overall assessment is over 50
      context has "crowdstrike" && context.crowdstrike.assessment.overall > 50
    )
    ||
    (
      // if Jamf data is present,
      // permit if Jamf's risk score is acceptable
      context has "jamf" && ["LOW", "NOT_APPLICABLE", "MEDIUM",
 "SECURE"].contains(context.jamf.risk)
    )
  )
};
```

Exemplos de políticas de acesso verificado

Exemplo 1: Criação de políticas para o IAM Identity Center

> **Note**
>
> Como os nomes dos grupos podem ser alterados, o IAM Identity Center se refere aos grupos usando seu ID de grupo. Isso ajuda a evitar a violação de uma declaração de política ao alterar o nome de um grupo.

O exemplo de política a seguir permite acesso somente quando um usuário pertence ao `finance` grupo (que tem ID de grupo de`c242c5b0-6081-1845-6fa8-6e0d9513c107`) e tem um endereço de e-mail verificado.

```
permit(principal,action,resource)
when {
    context.<policy-reference-name>.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
    && context.<policy-reference-name>.user.email.verified == true
};
```

Exemplo 1b: Adicionar mais condições a uma declaração de política do IAM Identity Center

O exemplo de política a seguir permite acesso somente quando um usuário pertence ao `finance` grupo (que tem um ID de grupo de `c242c5b0-6081-1845-6fa8-6e0d9513c107`), tem um endereço de e-mail verificado e a pontuação de risco do dispositivo Jamf é `LOW`.

```
permit(principal,action,resource)
when {
    context.<policy-reference-name>.groups has "c242c5b0-6081-1845-6fa8-6e0d9513c107"
    && context.<policy-reference-name>.user.email.verified == true
    && context.jamf.risk == "LOW"
};
```

Exemplo 2: A mesma política para um OIDC provedor terceirizado

O exemplo de política a seguir permite acesso somente quando o usuário é do grupo “financeiro”, tem um endereço de e-mail verificado e a pontuação de risco do dispositivo Jamf éLOW.

```
permit(principal,action,resource)
when {
     context.<policy-reference-name>.groups.contains("finance")
     && context.<policy-reference-name>.email_verified == true
     && context.jamf.risk == "LOW"
};
```

Exemplo 3: Usando CrowdStrike

O exemplo de política a seguir permite acesso quando a pontuação geral da avaliação é maior que 50.

```
permit(principal,action,resource)
when {
    context.crwd.assessment.overall > 50
};
```

Exemplo 4: adicionar tags com caracteres especiais

O exemplo a seguir mostra como escrever uma política se uma propriedade de contexto estiver usando um `:` (ponto e vírgula), que é um caractere reservado na linguagem da política.

```
permit(principal, action, resource)
```

```
when {
    context.<policy-reference-name>["namespace:groups"].contains("finance")
};
```

Exemplo 5: Permitir um endereço IP específico

O exemplo a seguir mostra uma política que permite somente um endereço IP específico.

```
permit(principal, action, resource)
when {
    context.http_request.client_ip == "192.0.2.1"
};
```

Exemplo 5a: Bloquear um endereço IP específico

O exemplo a seguir mostra uma política que bloqueará um endereço IP específico.

```
forbid(principal,action,resource)
when {
ip(context.http_request.client_ip).isInRange(ip("192.0.2.1/32"))
};
```

Assistente de políticas do Acesso Verificado

O assistente de políticas do Acesso Verificado é uma ferramenta no console do Acesso Verificado que você pode usar para testar e desenvolver as políticas. Ele apresenta a política de endpoint, a política de grupo e o contexto de confiança em uma tela, na qual você pode testar e editar as políticas.

Os formatos do contexto de confiança variam entre os diferentes provedores de confiança e, às vezes, o administrador do Acesso Verificado pode não saber o formato exato que um determinado provedor de confiança usa. É por isso que pode ser muito útil ver o contexto de confiança e as políticas de grupo e de endpoint em um só lugar para fins de teste e desenvolvimento.

As seções a seguir descrevem os princípios do uso do editor de políticas.

Tarefas

- Etapa 1: especificar os recursos
- Etapa 2: testar e editar as políticas

- Etapa 3: revisar e aplicar as alterações

Etapa 1: especificar os recursos

Na primeira página do assistente de políticas, especifique o endpoint do Acesso Verificado que você deseja usar. Especifique também um usuário (identificado pelo endereço de e-mail) e, opcionalmente, o nome do usuário e/ou um identificador do dispositivo. Por padrão, a decisão de autorização mais recente é extraída dos logs do Acesso Verificado do usuário especificado. Opcionalmente, você pode escolher especificamente a decisão mais recente de permissão ou negação.

Por fim, o contexto de confiança, a decisão de autorização, a política de endpoint e a política de grupo serão todos exibidos na próxima tela.

Para abrir o assistente de políticas e especificar seus recursos

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Instâncias do Acesso Verificado e clique no ID da instância do Acesso Verificado para a instância com a qual você deseja trabalhar.
3. Escolha Iniciar assistente de políticas.
4. Em Endereço de e-mail do usuário, insira o endereço de e-mail do usuário.
5. Em Endpoint do Acesso Verificado, selecione o endpoint para o qual você deseja editar e testar as políticas.
6. (Opcional) Em Nome, forneça o nome do usuário.
7. (Opcional) Em Identificador do dispositivo, forneça o identificador exclusivo do dispositivo.
8. (Opcional) Em Resultado da autorização, escolha o tipo de resultado da autorização recente que você deseja usar. Por padrão, o resultado da autorização mais recente será usado.
9. Escolha Próximo.

Etapa 2: testar e editar as políticas

Nesta página, você receberá as seguintes informações com as quais trabalhar:

- O contexto de confiança enviado pelo seu provedor de confiança para o usuário e (opcionalmente) para o dispositivo que você especificou na etapa anterior.
- A política do Cedar para o endpoint do Acesso Verificado especificada na etapa anterior.

- A política do Cedar para o grupo do Acesso Verificado ao qual o endpoint pertence.

As políticas do Cedar para o endpoint e o grupo do Acesso Verificado podem ser editadas nesta página, mas o contexto de confiança é estático. Agora você pode usar esta página para visualizar o contexto de confiança junto com as políticas do Cedar.

Teste as políticas em relação ao contexto de confiança escolhendo o botão Testar políticas e o resultado da autorização será exibido na tela. Você pode fazer edições nas políticas e testar novamente suas alterações, repetindo o processo conforme necessário.

Quando as alterações feitas nas políticas estiverem satisfatórias, escolha Avançar para continuar na próxima tela do assistente de políticas.

Etapa 3: revisar e aplicar as alterações

Na página final do assistente de políticas, as alterações feitas nas políticas serão destacadas para facilitar a revisão. Agora você pode revisar as políticas pela última vez e escolher Aplicar alterações para confirmá-las.

Você também tem a opção de voltar à página anterior escolhendo Anterior ou cancelar completamente o assistente de políticas escolhendo Cancelar.

Segurança no Acesso Verificado pela

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam ao Acesso AWS Verificado, consulte AWS Serviços no escopo do programa de conformidade AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Acesso Verificado. Os tópicos a seguir mostram como configurar o Acesso Verificado para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos de Acesso Verificado.

Conteúdo

Proteção de dados no Acesso Verificado

O modelo de responsabilidade AWS compartilhada de se aplica à proteção de dados no Acesso AWS Verificado. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre

seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre privacidade de dados, consulte Privacidade de dados FAQ. Para obter informações sobre proteção de dados na Europa, consulte o Modelo de Responsabilidade AWS Compartilhada e GDPR a postagem no blog AWS de segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use a autenticação multifator (MFA) com cada conta.
- UseSSL/TLSpara se comunicar com AWS os recursos. Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Configure API e registre as atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de FIPS 140-3 módulos criptográficos validados ao acessar AWS por meio de uma interface de linha de comando ou umaAPI, use um endpoint. FIPS Para obter mais informações sobre os FIPS endpoints disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com Acesso Verificado ou outro Serviços da AWS usando o console,API, AWS CLI, ou AWS SDKs. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é altamente recomendável que você não inclua informações de credenciais no URL para validar sua solicitação para esse servidor.

Criptografia em trânsito

O Acesso Verificado criptografa todos os dados em trânsito dos usuários finais para os pontos de extremidade do Acesso Verificado pela Internet usando o Transport Layer Security (TLS) 1.2 ou posterior.

Privacidade do tráfego entre redes

Você pode configurar o Acesso Verificado para restringir o acesso a recursos específicos em seuVPC. Para autenticação baseada no usuário, você também pode restringir o acesso a partes da rede, com base no grupo de usuários que acessa os endpoints. Para obter mais informações, consulte Políticas do Acesso Verificado.

Criptografia de dados em repouso para acesso AWS verificado

AWS O Verified Access criptografa dados em repouso por padrão, usando KMS chaves AWS próprias. Quando a criptografia de dados em repouso ocorre por padrão, ela ajuda a reduzir a sobrecarga operacional e a complexidade envolvidas na proteção de dados confidenciais. Ao mesmo tempo, ele permite que você crie aplicativos seguros que atendam aos rigorosos requisitos regulatórios e de conformidade de criptografia. As seções a seguir fornecem detalhes de como o Acesso Verificado usa KMS chaves para criptografia de dados em repouso.

Conteúdo

Acesso e KMS chaves verificados

AWS chaves de propriedade

O Acesso Verificado usa KMS chaves para criptografar automaticamente as informações de identificação pessoal (). PII Isso acontece por padrão, e você não pode visualizar, gerenciar, usar

ou auditar o uso das chaves de AWS propriedade. No entanto, não é necessário tomar nenhuma medida nem alterar qualquer programa para proteger as chaves que criptografam seus dados. Para obter mais informações, consulte chaves de propriedade da AWS no Guia do desenvolvedor do AWS Key Management Service .

Embora você não possa desabilitar essa camada de criptografia ou selecionar um tipo de criptografia alternativo, você pode adicionar uma segunda camada de criptografia sobre as chaves de criptografia de AWS propriedade existentes escolhendo uma chave gerenciada pelo cliente ao criar seus recursos de Acesso Verificado.

Chaves gerenciadas pelo cliente

O Acesso Verificado suporta o uso de chaves simétricas gerenciadas pelo cliente que você cria e gerencia para adicionar uma segunda camada de criptografia sobre a criptografia padrão existente. Como você tem controle total dessa camada de criptografia, você pode realizar tarefas como:

- Estabelecer e manter as políticas de chave
- Estabelecendo e mantendo IAM políticas e subsídios
- Habilitar e desabilitar políticas de chaves
- Alternar os materiais de criptografia de chave
- Adicionar etiquetas
- Criar réplicas de chaves
- Chaves de agendamento para exclusão

Para obter mais informações, consulte Chaves mestras do cliente (CMKs) no AWS Key Management Service Guia do desenvolvedor.

> **Note**
>
> O Acesso Verificado ativa automaticamente a criptografia em repouso usando chaves AWS próprias para proteger dados de identificação pessoal sem nenhum custo.
> No entanto, AWS KMS cobranças serão aplicadas quando você usar uma chave gerenciada pelo cliente. Para obter mais informações sobre a definição de preço, consulte Definição de preço do AWS Key Management Service.

Informações de identificação pessoal

A tabela a seguir resume as informações de identificação pessoal (PII) que o Acesso Verificado usa e como elas são criptografadas.

Tipo de dados	AWS criptografia de chave própria	Criptografia de chave gerenciada pelo cliente (opcional)
`Trust provider (user-type)` Os provedores de confiança do tipo usuário contêm OIDC opções como AuthorizationEndpoint, UserInfoEndpoint, ClientId ClientSecret, e assim por diante, que são consideradasPII.	Habilitado	Habilitado
`Trust provider (device-type)` Os provedores de confiança do tipo de dispositivo contêm um TenantId, que é considerado. PII	Habilitado	Habilitado
`Group policy` Fornecido durante a criação ou modificação do grupo de Acesso Verificado. Contém regras para autorizar solicitações de acesso. Pode conterPII, por exemplo, nome de usuário e endereço de e-mail, etc.	Habilitado	Habilitado

Tipo de dados	AWS criptografia de chave própria	Criptografia de chave gerenciada pelo cliente (opcional)
`Endpoint policy` Fornecido durante a criação ou modificação do endpoint de Acesso Verificado. Contém regras para autorizar solicitaç ões de acesso. Pode conterPII , por exemplo, nome de usuário e endereço de e-mail, etc.	Habilitado	Habilitado

Como o AWS Verified Access usa concessões em AWS KMS

O Acesso Verificado exige uma concessão para usar sua chave gerenciada pelo cliente.

Quando você cria recursos de Acesso Verificado criptografados com uma chave gerenciada pelo cliente, o Acesso Verificado cria uma concessão em seu nome enviando uma CreateGrantsolicitação para AWS KMS. As concessões AWS KMS são usadas para dar ao Acesso Verificado o acesso a uma chave gerenciada pelo cliente em sua conta.

O Acesso Verificado exige a concessão para usar sua chave gerenciada pelo cliente para as seguintes operações internas:

- Envie solicitações de descriptografia para AWS KMS descriptografar as chaves de dados criptografadas para que elas possam ser usadas para descriptografar seus dados.
- Envie RetireGrantsolicitações AWS KMS para excluir uma concessão.

É possível revogar o acesso à concessão, ou remover o acesso do serviço à chave gerenciada pelo cliente a qualquer momento. Se você fizer isso, o Acesso Verificado não poderá acessar nenhum dos dados criptografados pela chave gerenciada pelo cliente, o que afetará as operações que dependam desses dados.

Usar chaves gerenciadas pelo cliente com Acesso Verificado

Você pode criar uma chave simétrica gerenciada pelo cliente usando o AWS Management Console, ou o. AWS KMS APIs Siga as etapas para criar uma chave simétrica gerenciada pelo cliente no Guia do AWS Key Management Service desenvolvedor.

Políticas de chaves

As principais políticas controlam o acesso à chave gerenciada pelo cliente. Cada chave gerenciada pelo cliente deve ter exatamente uma política de chaves, que contém declarações que determinam quem pode usar a chave e como pode usá-la. Ao criar a chave gerenciada pelo cliente, você pode especificar uma política de chaves. Para obter mais informações, consulte Managing access to customer managed keys (Administrando o acesso a chaves gerenciadas pelo cliente) no Guia do desenvolvedor do AWS Key Management Service .

Para usar sua chave gerenciada pelo cliente com seus recursos de acesso verificado, as seguintes API operações devem ser permitidas na política de chaves:

- `kms:CreateGrant`: Adiciona uma concessão a uma chave gerenciada pelo cliente. Concede acesso de controle a uma KMS chave especificada, o que permite o acesso às operações de concessão exigidas pelo Acesso Verificado. Para obter mais informações, consulte Usar concessões no Guia do desenvolvedor do AWS Key Management Service .

  Isso permite que o Acesso Verificado faça o seguinte:

  - Ligue `GenerateDataKeyWithoutPlainText` para gerar uma chave de dados criptografada e armazená-la, porque a chave de dados não é usada imediatamente para criptografar.
  - Ligar para `Decrypt` para usar a chave de dados criptografada armazenada para acessar os dados criptografados.
  - Configure uma entidade principal aposentada para permitir que o serviço para `RetireGrant`.
- `kms:DescribeKey` : fornece os principais detalhes gerenciados pelo cliente para permitir que o serviço valide a chave.
- `kms:GenerateDataKey`: permite que o Acesso Verificado use a chave para criptografar dados.
- `kms:Decrypt`: permita que o Acesso Verificado descriptografe as chaves de dados criptografadas.

Veja a seguir um exemplo de política de chaves que você pode usar para Acesso Verificado.

```
"Statement" : [
```

```
    {
      "Sid" : "Allow access to principals authorized to use Verified Access",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "*"
      },
      "Action" : [
        "kms:DescribeKey",
        "kms:CreateGrant",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "kms:ViaService" : "verified-access.region.amazonaws.com",
          "kms:CallerAccount" : "111122223333"
        }
    },
    {
      "Sid": "Allow access for key administrators",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
       },
      "Action" : [
        "kms:*"
       ],
      "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
    },
    {
      "Sid" : "Allow read-only access to key metadata to the account",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "arn:aws:iam::111122223333:root"
      },
      "Action" : [
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "kms:RevokeGrant"
      ],
      "Resource" : "*"
    }
```

```
]
```

Para obter mais informações sobre Especificar permissões em uma política consulte o AWS Key Management Service Guia do desenvolvedor.

Para obter informações sobre acesso chave a solução de problemas , consulte AWS Key Management Service Guia do desenvolvedor.

Especificação de uma chave gerenciada pelo cliente para recursos de Acesso Verificado

Você pode especificar uma chave gerenciada pelo cliente para fornecer uma segunda camada de criptografia para os seguintes recursos:

- Grupo de Acesso Verificado
- Endpoint de Acesso Verificado
- Provedor confiável de Acesso Verificado

Ao criar qualquer um desses recursos usando o AWS Management Console, você pode especificar uma chave gerenciada pelo cliente na seção Criptografia adicional -- opcional. Durante o processo, marque a caixa de seleção Personalizar configurações de criptografia (avançadas) e insira a ID da AWS KMS chave que você deseja usar. Isso também pode ser feito ao modificar um recurso existente ou usando o AWS CLI.

> **Note**
>
> Se a chave gerenciada pelo cliente usada para adicionar criptografia adicional a qualquer um dos recursos acima for perdida, os valores de configuração dos recursos não estarão mais acessíveis. No entanto, os recursos podem ser modificados usando o AWS Management Console ou AWS CLI, para aplicar uma nova chave gerenciada pelo cliente e redefinir os valores de configuração.

AWS Contexto de criptografia de acesso verificado

Um contexto de criptografia é um conjunto opcional de pares de valores-chave que contêm informações contextuais adicionais sobre os dados. AWS KMS usa o contexto de criptografia como dados autenticados adicionais para oferecer suporte à criptografia autenticada. Quando você

inclui um contexto de criptografia em uma solicitação para criptografar dados, AWS KMS vincula o contexto de criptografia aos dados criptografados. Para descriptografar os dados, você inclui o mesmo contexto de criptografia na solicitação.

AWS Contexto de criptografia de acesso verificado

O Acesso Verificado usa o mesmo contexto de criptografia em todas as operações AWS KMS criptográficas, onde a chave está `aws:verified-access:arn` e o valor é o recurso Amazon Resource Name (ARN). Abaixo estão os contextos de criptografia dos recursos de Acesso Verificado.

Provedor confiável de Acesso Verificado

```
"encryptionContext": {
    "aws:verified-access:arn":
    "arn:aws:ec2:region:111122223333:VerifiedAccessTrustProviderId"
}
```

Grupo de Acesso Verificado

```
"encryptionContext": {
    "aws:verified-access:arn":
    "arn:aws:ec2:region:111122223333:VerifiedAccessGroupId"
}
```

Endpoint de Acesso Verificado

```
"encryptionContext": {
    "aws:verified-access:arn":
    "arn:aws:ec2:region:111122223333:VerifiedAccessEndpointId"
}
```

Para obter mais informações sobre o contexto de criptografia, consulte Contexto de criptografia no Guia do Desenvolvedor AWS Key Management Service .

Monitorando suas chaves de criptografia para acesso AWS verificado

Ao usar uma KMS chave gerenciada pelo cliente com seus recursos de Acesso AWS Verificado, você pode AWS CloudTrailusá-la para rastrear as solicitações enviadas pelo Acesso Verificado AWS KMS.

Os exemplos a seguir são AWS CloudTrail eventos para`CreateGrant`,`RetireGrant`, `DecryptDescribeKey`, e`GenerateDataKey`, que monitoram KMS as operações chamadas pelo Acesso Verificado para acessar dados criptografados pela KMS chave gerenciada pelo cliente:

CreateGrant

Quando você usa uma chave gerenciada pelo cliente para criptografar seus recursos, o Acesso Verificado envia uma `CreateGrant` solicitação em seu nome para acessar a chave em sua AWS conta. A concessão que o Acesso Verificado cria é específica para o recurso associado à chave gerenciada pelo cliente.

O evento de exemplo a seguir registra a operação `CreateGrant`:


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T16:27:12Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T16:41:42Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
```

```
    "requestParameters": {
        "operations": [
            "Decrypt",
            "RetireGrant",
            "GenerateDataKey"
        ],
        "keyId": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae",
        "constraints": {
            "encryptionContextSubset": {
                "aws:verified-access:arn": "arn:aws:ec2:ca-
central-1:111122223333:verified-access-trust-provider/vatp-0e54f581e2e5c97a2"
            }
        },
        "granteePrincipal": "verified-access.ca-central-1.amazonaws.com",
        "retiringPrincipal": "verified-access.ca-central-1.amazonaws.com"
    },
    "responseElements": {
        "grantId":
 "e5a050fff9893ba1c43f83fddf61e5f9988f579beaadd6d4ad6d1df07df6048f",
        "keyId": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae"
    },
    "requestID": "0faa837e-5c69-4189-9736-3957278e6444",
    "eventID": "1b6dd8b8-cbee-4a83-9b9d-d95fa5f6fd08",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


RetireGrant

O Acesso Verificado usa a `RetireGrant` operação para remover uma concessão quando você exclui um recurso.

O evento de exemplo a seguir registra a operação `RetireGrant`:


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T16:42:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T16:47:53Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RetireGrant",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": null,
    "responseElements": {
        "keyId": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae"
    },
    "additionalEventData": {
        "grantId":
 "b35e66f9bacb266cec214fcaa353c9cf750785e28773e61ba6f434d8c5c7632f"
    },
    "requestID": "7d4a31c2-d426-434b-8f86-336532a70462",
    "eventID": "17edc343-f25b-43d4-bbff-150d8fff4cf8",
    "readOnly": false,
```

```
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-central-1:111122223333:key/5ed79e7f-88c9-420c-
ae1a-61ee87104dae"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt

O Acesso Verificado chama a `Decrypt` operação para usar a chave de dados criptografada armazenada para acessar os dados criptografados.

O evento de exemplo a seguir registra a operação `Decrypt`:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T17:19:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
```

```
    },
    "eventTime": "2023-09-11T17:47:05Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e",
        "encryptionContext": {
            "aws:verified-access:arn": "arn:aws:ec2:ca-
central-1:111122223333:verified-access-trust-provider/vatp-00f20a4e455e9340f",
            "aws-crypto-public-key": "AkK+vi1W/
acBKv7OR8p2DeUrA8EgpTffSrjBqNucODuBYhyZ3hlMuYYJz9x7CwQWZw=="
        }
    },
    "responseElements": null,
    "requestID": "2e920fd3-f2f6-41b2-a5e7-2c2cb6f853a9",
    "eventID": "3329e0a3-bcfb-44cf-9813-8106d6eee31d",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


DescribeKey

O Acesso Verificado usa a `DescribeKey` operação para verificar se a chave gerenciada pelo cliente associada ao seu recurso existe na conta e na região.

O evento de exemplo a seguir registra a operação `DescribeKey`:


```
{
```

```
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T17:19:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T17:46:48Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
    },
    "responseElements": null,
    "requestID": "5b127082-6691-48fa-bfb0-4d40e1503636",
    "eventID": "ffcfc2bb-f94b-4c00-b6fb-feac77daff2a",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
        }
```

```
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateDataKey

O evento de exemplo a seguir registra a operação `GenerateDataKey`:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-11T17:19:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "verified-access.amazonaws.com"
    },
    "eventTime": "2023-09-11T17:46:49Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "verified-access.amazonaws.com",
    "userAgent": "verified-access.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
```

```
            "aws:verified-access:arn": "arn:aws:ec2:ca-
central-1:111122223333:verified-access-trust-provider/vatp-00f20a4e455e9340f",
            "aws-crypto-public-key": "A/ATGxaYatPUlOtM+l/mfDndkzHUmX5Hav+29IlIm
+JRBKFuXf24ulztmOIsqFQliw=="
        },
        "numberOfBytes": 32,
        "keyId": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
    },
    "responseElements": null,
    "requestID": "06535808-7cce-4ae1-ab40-e3afbf158a43",
    "eventID": "1ce79601-5a5e-412c-90b3-978925036526",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:ca-
central-1:111122223333:key/380d006e-706a-464b-99c5-68768297114e"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Gerenciamento de identidade e acesso para Acesso Verificado pela

AWS Identity and Access Management (IAM) é uma ferramenta Serviço da AWS que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. IAMos administradores controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar os recursos de acesso verificado. IAMé um Serviço da AWS que você pode usar sem custo adicional.

Tópicos

- Como o Acesso Verificado funciona com IAM
- Exemplos de políticas baseadas em identidade para Acesso Verificado pela
- Solução de problemas de identidade e acesso do Acesso Verificado pela
- Usar funções vinculadas ao serviço para o Acesso Verificado
- AWS políticas gerenciadas para acesso verificado

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Acesso Verificado.

Usuário do serviço: se você usa o serviço Acesso Verificado para fazer o trabalho, o administrador fornece as credenciais e as permissões necessárias. À medida que usar mais recursos do Acesso Verificado para fazer seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um recurso no Acesso Verificado, consulte Solução de problemas de identidade e acesso do Acesso Verificado pela .

Administrador do serviço: se você for o responsável pelos recursos do Acesso Verificado na empresa, provavelmente terá acesso total ao Acesso Verificado. Cabe a você determinar quais funcionalidades e recursos do Acesso Verificado os usuários do serviço devem acessar. Em seguida, você deve enviar solicitações ao IAM administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos doIAM. Para saber mais sobre como sua empresa pode usar IAM o Acesso Verificado, consulteComo o Acesso Verificado funciona com IAM.

IAMadministrador — Se você for IAM administrador, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao Acesso Verificado. Para ver exemplos de políticas baseadas em identidade de Acesso Verificado que você pode usar emIAM, consulte. Exemplos de políticas baseadas em identidade para Acesso Verificado pela

Autenticando com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como IAM usuário ou assumindo uma IAM função. Usuário raiz da conta da AWS

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Os usuários (do IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você entra como uma identidade federada, seu administrador configurou previamente a federação de identidades usando IAM funções. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para você mesmo assinar solicitações, consulte Assinar AWS API solicitações no Guia IAM do usuário.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia AWS IAM Identity Center do usuário e Uso da autenticação multifator (MFA) AWS no Guia do IAMusuário.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para ver a lista completa de tarefas que exigem que você faça login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do IAM usuário.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter informações sobre o IAM Identity Center, consulte O que é o IAM Identity Center? no Guia do AWS IAM Identity Center usuário.

Grupos e usuários do IAM

Um IAMusuário é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos confiar em credenciais temporárias em vez de criar IAM usuários que tenham credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com IAM os usuários, recomendamos que você alterne as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exigem credenciais de longo prazo no Guia do IAMusuário.

Um IAMgrupo é uma identidade que especifica uma coleção de IAM usuários. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar IAM recursos.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um IAM usuário (em vez de uma função) no Guia do IAM usuário.

IAMfunções

Uma IAMfunção é uma identidade dentro da sua Conta da AWS que tem permissões específicas. É semelhante a um IAM usuário, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma IAM função no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma AWS API operação AWS CLI or ou usando uma

personalizadaURL. Para obter mais informações sobre métodos de uso de funções, consulte Usando IAM funções no Guia IAM do usuário.

IAMfunções com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter informações sobre funções para federação, consulte Criação de uma função para um provedor de identidade terceirizado no Guia IAM do usuário. Se você usa o IAM Identity Center, configura um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a uma função em. IAM Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .
- Permissões temporárias IAM de IAM usuário — Um usuário ou função pode assumir uma IAM função para assumir temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas — Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um Serviço da AWS, combinadas com a solicitação Serviço da AWS para fazer solicitações aos serviços posteriores. FASas solicitações são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte Encaminhar sessões de acesso.

  - Função de serviço — Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma Serviço da AWS no Guia do IAM usuário.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. Serviço da AWS O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.
- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo AWS CLI AWS API solicitações. Isso é preferível ao armazenamento de chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que os programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Como usar uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia IAM do usuário.

Para saber se usar IAM funções ou IAM usuários, consulte Quando criar uma IAM função (em vez de um usuário) no Guia do IAM usuário.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como JSON documentos. Para obter mais informações sobre a estrutura e o conteúdo dos documentos de JSON política, consulte Visão geral das JSON políticas no Guia IAM do usuário.

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O

administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

IAMas políticas definem permissões para uma ação, independentemente do método usado para realizar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função do AWS Management Console AWS CLI, do ou do AWS API.

Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de IAM políticas no Guia do IAMusuário.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolha entre políticas gerenciadas e políticas em linha no Guia do IAMusuário.

Políticas baseadas no recurso

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas de uma política baseada IAM em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLssão semelhantes às políticas baseadas em recursos, embora não usem o formato de documento JSON de política.

Amazon S3, AWS WAF, e Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber maisACLs, consulte a visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões — Um limite de permissões é um recurso avançado no qual você define as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (IAMusuário ou função). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para IAM entidades no Guia IAM do usuário.
- Políticas de controle de serviço (SCPs) — SCPs são JSON políticas que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. Os SCP limites de permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations eSCPs, consulte Políticas de controle de serviços no Guia AWS Organizations do Usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas

substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia IAM do usuário.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de política estão envolvidos, consulte Lógica de avaliação de políticas no Guia IAM do usuário.

Como o Acesso Verificado funciona com IAM

Antes de usar IAM para gerenciar o acesso ao Acesso Verificado, saiba quais IAM recursos estão disponíveis para uso com o Acesso Verificado.

IAMrecurso	Suporta Acesso Verificado
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim
Atributos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC(tags nas políticas)	Parcial
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Sim

Para ter uma visão geral de como o Acesso Verificado e outros AWS serviços funcionam com a maioria dos IAM recursos, consulte AWS os serviços que funcionam com IAM no Guia do IAM Usuário.

Políticas baseadas em identidade para Acesso Verificado

Compatível com políticas baseadas em identidade: Sim

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de IAM políticas no Guia do IAMusuário.

Com políticas IAM baseadas em identidade, você pode especificar ações e recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que você pode usar em uma JSON política, consulte a referência IAM JSON de elementos de política no Guia IAM do usuário.

Exemplos de políticas baseadas em identidade para Acesso Verificado

Para visualizar exemplos de políticas baseadas em identidade do Acesso Verificado, consulte Exemplos de políticas baseadas em identidade para Acesso Verificado pela .

Políticas baseadas em recursos no Acesso Verificado

Suporte a políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para habilitar o acesso entre contas, você pode especificar uma conta ou IAM entidades inteiras em outra conta como principal em uma política baseada em recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um IAM administrador na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

Ações políticas para Acesso Verificado

Compatível com ações de políticas: Sim

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O `Action` elemento de uma JSON política descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da AWS API operação associada. Há algumas exceções, como ações somente de permissão que não têm uma operação correspondente. API Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações de acesso verificado, consulte Ações definidas pela Amazon EC2 na Referência de autorização de serviço.

As ações de políticas no Acesso Verificado usam o seguinte prefixo antes da ação:

```
ec2
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

```
"Action": [
    "ec2:action1",
    "ec2:action2"
]
```

Para visualizar exemplos de políticas baseadas em identidade do Acesso Verificado, consulte Exemplos de políticas baseadas em identidade para Acesso Verificado pela .

Recursos de política para Acesso Verificado

Compatível com recursos de políticas: Sim

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Resource` JSON de política especifica o objeto ou objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu Amazon Resource Name (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de recursos de acesso verificado e seusARNs, consulte Recursos definidos pela Amazon EC2 na Referência de autorização de serviço. Para saber com quais ações você pode especificar cada recurso, consulte Ações definidas pela Amazon EC2. ARN

Para visualizar exemplos de políticas baseadas em identidade do Acesso Verificado, consulte Exemplos de políticas baseadas em identidade para Acesso Verificado pela .

Chaves de condição da política do Acesso Verificado

Compatível com chaves de condição de política específicas de serviço: Sim

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões

condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, você pode conceder permissão a um IAM usuário para acessar um recurso somente se ele estiver marcado com o nome de IAM usuário. Para obter mais informações, consulte elementos de IAM política: variáveis e tags no Guia IAM do usuário.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia IAM do usuário.

Para ver uma lista de chaves de condição de acesso verificado, consulte Chaves de condição da Amazon EC2 na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pela Amazon EC2.

Para visualizar exemplos de políticas baseadas em identidade do Acesso Verificado, consulte Exemplos de políticas baseadas em identidade para Acesso Verificado pela .

ACLsem Acesso verificado

SuportesACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLssão semelhantes às políticas baseadas em recursos, embora não usem o formato de documento JSON de política.

ABACcom acesso verificado

Suportes ABAC (tags nas políticas): Parciais

O controle de acesso baseado em atributos (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a IAM entidades (usuários ou funções) e a muitos AWS recursos. Marcar entidades e

recursos é a primeira etapa doABAC. Em seguida, você cria ABAC políticas para permitir operações quando a tag do diretor corresponde à tag do recurso que ele está tentando acessar.

ABACé útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna complicado.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobreABAC, consulte O que éABAC? no Guia do IAM usuário. Para ver um tutorial com etapas de configuraçãoABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do IAMusuário.

Usar credenciais temporárias com Acesso Verificado

Compatível com credenciais temporárias: Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS esse trabalho IAM no Guia do IAM usuário.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre a troca de funções, consulte Alternando para uma função (console) no Guia IAM do usuário.

Você pode criar manualmente credenciais temporárias usando o AWS CLI ou AWS API. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias emIAM.

Permissões de entidade principal entre serviços para o Acesso Verificado

Suporta sessões de acesso direto (FAS): Sim

Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um Serviço da AWS, combinadas com a solicitação Serviço da AWS para fazer solicitações aos serviços posteriores. FASas solicitações são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte Encaminhar sessões de acesso.

Perfis de serviço para Acesso Verificado

Compatível com perfis de serviço: não

Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma Serviço da AWS no Guia do IAM usuário.

Perfis vinculados ao serviço para Acesso Verificado

Suporte a perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. Serviço da AWS O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas ao serviço do Acesso Verificado, consulte Usar funções vinculadas ao serviço para o Acesso Verificado.

Exemplos de políticas baseadas em identidade para Acesso Verificado pela

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do ACM. Eles também não podem realizar tarefas usando o AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

Para saber como criar uma política IAM baseada em identidade usando esses exemplos de documentos de JSON política, consulte Criação de IAM políticas no Guia do IAMusuário.

Para obter detalhes sobre ações e tipos de recursos definidos pelo Verified Access, incluindo o formato ARNs de cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para a Amazon EC2 na Referência de autorização de serviço.

Tópicos

- Melhores práticas de política
- Política para criar instâncias de Acesso Verificado
- Permitir que usuários visualizem suas próprias permissões

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Acesso Verificado em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte políticas AWS gerenciadas ou políticas AWS gerenciadas para funções de trabalho no Guia IAM do usuário.
- Aplique permissões com privilégios mínimos — Ao definir permissões com IAM políticas, conceda somente as permissões necessárias para realizar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre IAM como usar para aplicar permissões, consulte Políticas e permissões IAM no Guia IAM do usuário.
- Use condições nas IAM políticas para restringir ainda mais o acesso — Você pode adicionar uma condição às suas políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usandoSSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica Serviço da AWS, como AWS CloudFormation. Para obter mais informações, consulte Elementos IAM JSON da política: Condição no Guia IAM do usuário.
- Use o IAM Access Analyzer para validar suas IAM políticas e garantir permissões seguras e funcionais — o IAM Access Analyzer valida políticas novas e existentes para que as políticas

sigam a linguagem da IAM política (JSON) e as melhores práticas. IAM IAMO Access Analyzer fornece mais de 100 verificações de políticas e recomendações práticas para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação da política do IAM Access Analyzer no Guia do IAM Usuário.

- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija IAM usuários ou um usuário root Conta da AWS, ative MFA para obter segurança adicional. Para exigir MFA quando API as operações são chamadas, adicione MFA condições às suas políticas. Para obter mais informações, consulte Configurando o API acesso MFA protegido no Guia do IAMusuário.

Para obter mais informações sobre as melhores práticas emIAM, consulte as melhores práticas de segurança IAM no Guia IAM do usuário.

Política para criar instâncias de Acesso Verificado

Para criar uma instância de acesso verificado, IAM os diretores precisam adicionar essa declaração adicional à IAM política.

```
{
    "Effect": "Allow",
    "Action": "verified-access:AllowVerifiedAccess",
    "Resource": "*"
}
```

> **Note**
>
> `verified-access:AllowVerifiedAccess`é um ambiente virtual somente para ação. API Ele não oferece suporte à autorização baseada em chave de recurso, tag ou condição. Use autorização baseada em recurso, tag ou chave de condição na ação `ec2:CreateVerifiedAccessInstance`API.

Exemplo de política para criar uma instância do Acesso Verificado. Neste exemplo, `123456789012` é o número da AWS conta e `us-east-1` é a AWS região.

```
{
      "Version": "2012-10-17",
      "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": "ec2:CreateVerifiedAccessInstance",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:verified-access-instance/*"
        },
        {
            "Effect": "Allow",
            "Action": "verified-access:AllowVerifiedAccess",
            "Resource": "*"
        }
    ]
}
```

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permita IAM aos usuários visualizar as políticas embutidas e gerenciadas que estão anexadas à identidade do usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando o AWS CLI ou. AWS API

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
```

```
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Solução de problemas de identidade e acesso do Acesso Verificado pela

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o Acesso Verificado e. IAM

Problemas

- Não tenho autorização para executar uma ação no Acesso Verificado
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos de Acesso Verificado

Não tenho autorização para executar uma ação no Acesso Verificado

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O exemplo de erro a seguir ocorre quando o `mateojackson` IAM usuário tenta usar o console para ver detalhes sobre um *`my-example-widget`* recurso fictício, mas não tem as permissões fictícias`ec2:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `ec2:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, as suas políticas deverão ser atualizadas para permitir a passagem de um perfil para o Acesso Verificado.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um IAM usuário chamado `marymajor` tenta usar o console para realizar uma ação no Acesso Verificado. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos de Acesso Verificado

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte o seguinte:

- Para saber se o Acesso Verificado oferece suporte a esses recursos, consulte Como o Acesso Verificado funciona com IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Fornecer acesso a um IAM usuário em outro Conta da AWS de sua propriedade no Guia do IAM usuário.

- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Fornecer Contas da AWS acesso a terceiros no Guia do IAM usuário.
- Para saber como fornecer acesso por meio da federação de identidades, consulte Fornecendo acesso a usuários autenticados externamente (federação de identidades) no Guia do IAMusuário.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

Usar funções vinculadas ao serviço para o Acesso Verificado

Acesso Verificado pela AWS usa AWS Identity and Access Management (IAM) funções vinculadas ao serviço. Uma função vinculada ao serviço é um tipo exclusivo de IAM função vinculada diretamente ao Acesso Verificado. As funções vinculadas ao serviço são predefinidas pelo Acesso Verificado e incluem todas as permissões que o serviço exige para ligar para outras pessoas Serviços da AWS em seu nome.

Um perfil vinculado ao serviço facilita a configuração do Acesso Verificado porque não é preciso adicionar as permissões necessárias manualmente. O Acesso Verificado define as permissões das funções vinculadas ao serviço e, exceto se definido de outra forma, somente o Access Analyzer pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política de permissões não pode ser anexada a nenhuma outra IAM entidade.

Para obter informações sobre outros serviços que oferecem suporte a funções vinculadas a serviços, consulte AWS serviços que funcionam com IAM e procure os serviços que têm Sim na coluna Funções vinculadas ao serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões de perfil vinculado ao serviço para detecção de conta do Acesso Verificado

O Acesso Verificado usa a função vinculada ao serviço nomeada AWSServiceRoleForVPCVerifiedAccesspara provisionar recursos em sua conta que são necessários para usar o serviço.

A função AWSServiceRoleForVPCVerifiedAccessvinculada ao serviço confia nos seguintes serviços para assumir a função:

- `verified-access.amazonaws.com`

A política de permissões de função, denominada AWSVPCVerifiedAccessServiceRolePolicy, permite que o Acesso Verificado conclua as seguintes ações nos recursos especificados:

- Ação `ec2:CreateNetworkInterface` em todas as sub-redes e grupos de segurança, bem como em todas as interfaces de rede com a tag `VerifiedAccessManaged=true`
- Ação `ec2:CreateTags` em todas as interfaces de rede no momento da criação
- Ação `ec2:DeleteNetworkInterface` em todas as interfaces de rede com a tag `VerifiedAccessManaged=true`
- Ação `ec2:ModifyNetworkInterfaceAttribute` em todos os grupos de segurança e todas as interfaces de rede com a tag `VerifiedAccessManaged=true`

Você também pode ver as permissões dessa política no AWS Management Console AWSVPCVerifiedAccessServiceRolePolicy, ou você pode ver a AWSVPCVerifiedAccessServiceRolePolicypolítica no Guia de referência de políticas AWS gerenciadas.

Você deve configurar permissões para permitir que uma IAM entidade (como usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Permissões de funções vinculadas ao serviço no Guia do IAMusuário.

Criar um perfil vinculado ao serviço para o Acesso Verificado

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você chama CreateVerifiedAccessEndpointo AWS Management Console, o ou o AWS CLI AWS API, o Acesso Verificado cria a função vinculada ao serviço para você.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você poderá usar esse mesmo processo para recriar a função em sua conta. Quando você liga CreateVerifiedAccessEndpointnovamente, o Acesso Verificado cria a função vinculada ao serviço para você novamente.

Editar um perfil vinculado ao serviço para o Acesso Verificado

O Acesso Verificado não permite que você edite a função AWSServiceRoleForVPCVerifiedAccessvinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, você pode editar a descrição da função usandoIAM. Para obter mais informações, consulte Edição de uma função vinculada ao serviço no Guia do IAMusuário.

Excluir um perfil vinculado ao serviço para o Acesso Verificado

Você não precisa excluir manualmente a AWSServiceRoleForVPCVerifiedAccessfunção. Quando você chama DeleteVerifiedAccessEndpointo AWS Management Console, o ou o AWS CLI AWS API, o Acesso Verificado limpa os recursos e exclui a função vinculada ao serviço para você.

Para excluir manualmente a função vinculada ao serviço usando IAM

Use o IAM console AWS CLI, o ou o AWS API para excluir a função AWSServiceRoleForVPCVerifiedAccessvinculada ao serviço. Para obter mais informações, consulte Excluindo uma função vinculada ao serviço no Guia do IAM usuário.

Regiões compatíveis com perfis vinculados ao serviço do Acesso Verificado

O Acesso Verificado oferece suporte ao uso de funções vinculadas ao serviço em todos os lugares em Regiões da AWS que o serviço está disponível. Para obter mais informações, consulte Regiões e endpoints da AWS.

AWS políticas gerenciadas para acesso verificado

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova Serviço da AWS é lançada ou novas API operações são disponibilizadas para os serviços existentes.

Para obter mais informações, consulte as políticas AWS gerenciadas no Guia IAM do usuário.

AWS política gerenciada: AWSVPCVerifiedAccessServiceRolePolicy

Esta política está anexada a um perfil vinculado ao serviço que permite ao Acesso Verificado executar ações em seu nome. Para obter mais informações, consulte Usar

perfis vinculados a serviços. Para ver as permissões dessa política, você pode ver AWSVPCVerifiedAccessServiceRolePolicyno AWS Management Console, ou você pode ver a AWSVPCVerifiedAccessServiceRolePolicypolítica no Guia de referência de políticas AWS gerenciadas.

Atualizações de acesso verificado às políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Acesso Verificado desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o RSS feed na página de histórico do Documento de Acesso Verificado.

Alteração	Descrição	Data
AWSVPCVerifiedAccessServiceRolePolicy- Política atualizada	O Verified Access atualizou sua política gerenciada para incluir descrições de todas as ações no campo “sid”.	17 de novembro de 2023
AWSVPCVerifiedAccessServiceRolePolicy- Política atualizada	O Verified Access atualizou sua política gerenciada para adicionar recursos de grupo de segurança à `ec2:CreateNetworkInterface` permissão.	31 de maio de 2023
AWSVPCVerifiedAccessServiceRolePolicy- Nova política	O Acesso Verificado adicionou uma nova política para permitir provisionar recursos em sua conta que são necessários para usar o serviço.	29 de novembro de 2022
O Acesso Verificado começou a monitorar as alterações	O Verified Access começou a rastrear as alterações em suas políticas AWS gerenciadas.	29 de novembro de 2022

Validação de conformidade do Acesso Verificado pela

Acesso Verificado pela AWS pode ser configurado para suportar a conformidade com os Padrões Federais de Processamento de Informações (FIPS). Para obter mais informações e detalhes sobre como configurar a FIPS conformidade do Acesso Verificado, acesseFIPSconformidade com o Verified Access.

Para saber se um Serviço da AWS está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para HIPAA segurança e conformidade na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar HIPAA aplicativos qualificados.

> **Note**
>
> Nem todos Serviços da AWS são HIPAA elegíveis. Para obter mais informações, consulte a Referência de serviços HIPAA elegíveis.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização ()). ISO

- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso Serviço da AWS fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso Serviço da AWS detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, por exemplo PCIDSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso Serviço da AWS ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência no Acesso Verificado pela

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicativos e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Além da infraestrutura AWS global, o Verified Access oferece o seguinte recurso para ajudar a atender às suas necessidades de alta disponibilidade.

Várias sub-redes para alta disponibilidade

Ao criar um endpoint de Acesso Verificado do tipo balanceador de carga, você pode associar várias sub-redes ao endpoint. Cada sub-rede que você associa ao endpoint deve pertencer a uma zona

de disponibilidade diferente. Ao associar várias sub-redes, você pode garantir alta disponibilidade usando várias zonas de disponibilidade.

Monitoramento Acesso Verificado pela AWS

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do Acesso Verificado pela AWS. AWS fornece as seguintes ferramentas de monitoramento para monitorar o Acesso Verificado, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- Logs de acesso: capture informações detalhadas sobre solicitações de acesso a aplicativos. Para obter mais informações, consulte the section called “Logs de Verified Acesss”.
- AWS CloudTrail— Captura API chamadas e eventos relacionados feitos por você ou em seu nome Conta da AWS e entrega os arquivos de log em um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte the section called “CloudTrail troncos”.

Logs de Verified Acesss

Depois de Acesso Verificado pela AWS avaliar cada solicitação de acesso, ela registra todas as tentativas de acesso. Isso fornece visibilidade centralizada do acesso aos aplicativos e ajuda você a responder rapidamente a incidentes de segurança e solicitações de auditoria. O Verified Access suporta o formato de registro do Open Cybersecurity Schema Framework (OCSF).

Ao ativar o registro, você precisa configurar um destino para o envio dos registros. O IAM principal usado para configurar o destino do registro precisa ter certas permissões para que o registro funcione corretamente. As IAM permissões necessárias para cada destino de registro podem ser vistas na Permissões de registro de acesso verificadas seção. O Acesso Verificado oferece suporte aos seguintes destinos para publicação de logs de acesso:

- Grupos CloudWatch de registros do Amazon Logs
- Buckets do Amazon S3
- Streams de entrega do Amazon Data Firehose

Conteúdo

- Ativar ou desativar registros de acesso verificado
- Ativar ou desativar o contexto de confiança do Acesso Verificado
- OCSFexemplos de log da versão 0.1 para acesso verificado
- OCSFexemplos de log da versão 1.0.0-rc.2 para acesso verificado

Versões de registro de acesso verificadas

Por padrão, o sistema de registro de acesso verificado usa o Open Cybersecurity Schema Framework (OCSF) versão 0.1. Exemplos de logs usando a versão 0.1 podem ser vistos na seção OCSFexemplos de log da versão 0.1 para acesso verificado.

A versão de registro mais recente é compatível com a OCSF versão 1.0.0-rc.2. Detalhes específicos sobre o esquema podem ser encontrados aqui OCSFEsquema. Exemplos de logs usando a versão 1.0.0-rc.2 podem ser vistos na seção OCSFexemplos de log da versão 1.0.0-rc.2 para acesso verificado.

Se você quiser atualizar a versão de registro que está sendo usada, use o procedimento a seguir.

Para atualizar a versão de log usando o console

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do Acesso Verificado.
3. Selecione a instância de Acesso Verificado apropriada.
4. Na guia Configuração de log de instância de Acesso Verificado, escolha Modificar configuração de log de instância de Acesso Verificado.
5. Selecione ocsf-1.0.0-rc.2 na lista suspensa Versão do log de atualização.
6. Escolha Modificar configuração de log da instância de Acesso Verificado.

Para atualizar a versão de registro usando o AWS CLI

Use o comando modify-verified-access-instance-logging-configuration.

Permissões de registro de acesso verificadas

O IAM principal usado para configurar o destino do registro precisa ter certas permissões para que o registro funcione corretamente. As seções a seguir mostram as permissões necessárias para cada destino de registro.

Para entrega ao CloudWatch Logs:

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration` na instância de Acesso Verificado
- `logs:CreateLogDelivery`, `logs:DeleteLogDelivery`, `logs:GetLogDelivery`, `logs:ListLogDeliveries` e `logs:UpdateLogDelivery` em todos os recursos
- `logs:DescribeLogGroups`, `logs:DescribeResourcePolicies`, e `logs:PutResourcePolicy` no grupo de logs de destino

Para entrega no Amazon S3:

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration` na instância de Acesso Verificado
- `logs:CreateLogDelivery`, `logs:DeleteLogDelivery`, `logs:GetLogDelivery`, `logs:ListLogDeliveries` e `logs:UpdateLogDelivery` em todos os recursos
- `s3:GetBucketPolicy` e `s3:PutBucketPolicy` no bucket de destino

Para entrega ao Firehose:

- `ec2:ModifyVerifiedAccessInstanceLoggingConfiguration` na instância de Acesso Verificado
- `firehose:TagDeliveryStream` Para todos os recursos
- `iam:CreateServiceLinkedRole` Para todos os recursos
- `logs:CreateLogDelivery`, `logs:DeleteLogDelivery`, `logs:GetLogDelivery`, `logs:ListLogDeliveries` e `logs:UpdateLogDelivery` em todos os recursos

Ativar ou desativar registros de acesso verificado

Você pode usar os procedimentos nesta seção para ativar ou desativar o registro. Ao ativar o registro, você precisa configurar um destino para o envio dos registros. O IAM principal usado para configurar o destino do registro precisa ter certas permissões para que o registro funcione corretamente. As IAM permissões necessárias para cada destino de registro podem ser vistas na Permissões de registro de acesso verificadas seção.

Conteúdo

- Habilitar logs de acesso
- Desabilitar logs de acesso

Habilitar logs de acesso

Para habilitar logs de Acesso Verificado

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do Acesso Verificado.
3. Selecione a instância de Acesso Verificado.
4. Na guia Configuração de log de instância de Acesso Verificado, escolha Modificar configuração de log de instância de Acesso Verificado.
5. (Opcional) Para incluir dados de confiança enviados de provedores confiáveis nos logs, faça o seguinte:
   a. Selecione ocsf-1.0.0-rc.2 na lista suspensa Versão do log de atualização.
   b. Escolha Incluir contexto de confiança.
6. Faça um dos seguintes procedimentos:
   - Ative a opção Entregar para Amazon CloudWatch Logs. Escolha o grupo de logs de destino.
   - Ative a opção Entregar para o Amazon S3. Insira o nome, o proprietário e o prefixo do bucket de destino.
   - Ative o Deliver to Firehose. Escolha o fluxo de entrega de destino.
7. Escolha Modificar configuração de log da instância de Acesso Verificado.

Para ativar os registros de acesso verificado usando o AWS CLI

Use o comando modify-verified-access-instance-logging-configuration.

Desabilitar logs de acesso

Você pode desativar os logs de acesso da sua instância de Acesso Verificado a qualquer momento. Depois que os logs de acesso forem desabilitados, seus dados permanecerão no destino até que você os exclua.

Para desabilitar os logs de Acesso Verificado

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do Acesso Verificado.
3. Selecione a instância de Acesso Verificado.
4. Na guia Configuração de log de instância de Acesso Verificado, escolha Modificar configuração de log de instância de Acesso Verificado.
5. Desative a entrega de logs.
6. Escolha Modificar configuração de log da instância de Acesso Verificado.

Para desativar os registros de acesso verificado usando o AWS CLI

Use o comando modify-verified-access-instance-logging-configuration.

Ativar ou desativar o contexto de confiança do Acesso Verificado

O contexto de confiança enviado pelo seu provedor de confiança pode, opcionalmente, ser ativado para inclusão em seus registros de acesso verificado. Isso pode ser útil ao definir políticas que permitem ou negam acesso aos seus aplicativos. Depois de habilitá-lo, o contexto de confiança é encontrado no registro abaixo do `data` campo. Se o contexto de confiança estiver desativado, o `data` campo será definido como`null`. Para configurar o Acesso Verificado para incluir contexto de confiança nos registros, siga o procedimento a seguir.

> **Note**
>
> A inclusão do contexto de confiança em seus logs de Acesso Verificado exige a atualização para a versão `ocsf-1.0.0-rc.2` mais recente do log. O procedimento a seguir pressupõe que você já tenha o registro ativado. Se isso não for verdade, consulte Habilitar logs de acesso o procedimento completo.

Conteúdo

Habilitar contexto de confiança

Para incluir contexto de confiança nos logs de Acesso Verificado usando o console

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do Acesso Verificado.
3. Selecione a instância de Acesso Verificado apropriada.
4. Na guia Configuração de log de instância de Acesso Verificado, escolha Modificar configuração de log de instância de Acesso Verificado.
5. Selecione ocsf-1.0.0-rc.2 na lista suspensa Versão do log de atualização.
6. Ative a opção Incluir contexto de confiança.
7. Escolha Modificar configuração de log da instância de Acesso Verificado.

Para incluir contexto de confiança nos registros de acesso verificado usando o AWS CLI

Use o comando modify-verified-access-instance-logging-configuration.

Desabilitar contexto de confiança

Se você não quiser mais incluir o contexto de confiança nos registros, poderá removê-lo seguindo o procedimento a seguir.

Para remover o contexto de confiança dos logs de Acesso Verificado usando o console

1. Abra o VPC console da Amazon em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, selecione Instâncias do Acesso Verificado.
3. Selecione a instância de Acesso Verificado apropriada.
4. Na guia Configuração de log de instância de Acesso Verificado, escolha Modificar configuração de log de instância de Acesso Verificado.
5. Desative a opção Incluir contexto de confiança.
6. Escolha Modificar configuração de log da instância de Acesso Verificado.

Para remover o contexto de confiança dos registros de acesso verificado usando o AWS CLI

Use o comando modify-verified-access-instance-logging-configuration.

OCSFexemplos de log da versão 0.1 para acesso verificado

Veja a seguir exemplos de registros usando a OCSF versão de registro padrão 0.1.

Exemplos

Acesso concedido com OIDC

Neste exemplo de entrada de registro, o Acesso Verificado permite acesso a um endpoint com um provedor confiável OIDC do usuário.


```
{
    "activity": "Access Granted",
    "activity_id": "1",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": {
        "ip": "10.2.7.68",
        "type": "Unknown",
        "type_id": 0
    },
    "duration": "0.004",
    "end_time": "1668580194344",
    "time": "1668580194344",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "https",
            "text": "https://hello.app.example.com:443/"
```

```
        },
        "user_agent": "python-requests/2.28.1",
        "version": "HTTP/1.1"
    },
    "http_response": {
        "code": 200
    },
    "identity": {
        "authorizations": [
            {
                "decision": "Allow",
                "policy": {
                    "name": "inline"
                }
            }
        ],
        "idp": {
            "name": "user",
            "uid": "vatp-09bc4cbce2EXAMPLE"
        },
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "00u6wj48lbxTAEXAMPLE"
        }
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-63748362-6408d24241120b942EXAMPLE",
        "logged_time": 1668580281337,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T06:29:54.344948Z",
    "proxy": {
        "ip": "192.168.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-002fa341aeEXAMPLE"
    },
```

```
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "172.24.57.68",
        "port": "48234"
    },
    "start_time": "1668580194340",
    "status_code": "100",
    "status_details": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "20800101",
    "type_name": "AccessLogs: Access Granted",
    "unmapped": null
}
```

Acesso concedido com OIDC e JAMF

Neste exemplo de entrada de registro, o Acesso Verificado permite acesso a um endpoint com provedores confiáveis OIDC e de JAMF dispositivos.

```
{
    "activity": "Access Granted",
    "activity_id": "1",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": {
        "ip": "10.2.7.68",
        "type": "Unknown",
        "type_id": 0,
        "uid": "41b07859-4222-4f41-f3b9-97dc1EXAMPLE"
    },
    "duration": "0.347",
    "end_time": "1668804944086",
    "time": "1668804944086",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
```

```
            "scheme": "h2",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36",
        "version": "HTTP/2.0"
    },
    "http_response": {
        "code": 304
    },
    "identity": {
        "authorizations": [
            {
                "decision": "Allow",
                "policy": {
                    "name": "inline"
                }
            }
        ],
        "idp": {
            "name": "oidc",
            "uid": "vatp-9778003bc2EXAMPLE"
        },
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "4f040d0f96becEXAMPLE"
        }
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-321318ce-6100d340adf4fb29dEXAMPLE",
        "logged_time": 1668805278555,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-18T20:55:44.086480Z",
    "proxy": {
        "ip": "10.5.192.96",
        "port": 443,
```

```
        "svc_name": "Verified Access",
        "uid": "vai-3598f66575EXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "192.168.20.246",
        "port": 61769
    },
    "start_time": "1668804943739",
    "status_code": "100",
    "status_details": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "20800101",
    "type_name": "AccessLogs: Access Granted",
    "unmapped": null
}
```

Acesso concedido com OIDC e CrowdStrike

Neste exemplo de entrada de registro, o Acesso Verificado permite acesso a um endpoint com provedores confiáveis OIDC e de CrowdStrike dispositivos.

```
{
    "activity": "Access Granted",
    "activity_id": "1",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": {
        "ip": "10.2.173.3",
        "os": {
            "name": "Windows 11",
            "type": "Windows",
            "type_id": 100
        },
        "type": "Unknown",
        "type_id": 0,
        "uid": "122978434f65093aee5dfbdc0EXAMPLE",
        "hw_info": {
            "serial_number": "751432a1-d504-fd5e-010d-5ed11EXAMPLE"
```

```
        }
    },
    "duration": "0.028",
    "end_time": "1668816620842",
    "time": "1668816620842",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "test.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "h2",
            "text": "https://test.app.example.com:443/"
        },
        "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36",
        "version": "HTTP/2.0"
    },
    "http_response": {
        "code": 304
    },
    "identity": {
        "authorizations": [
            {
                "decision": "Allow",
                "policy": {
                    "name": "inline"
                }
            }
        ],
        "idp": {
            "name": "oidc",
            "uid": "vatp-506d9753f6EXAMPLE"
        },
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "23bb45b16a389EXAMPLE"
        }
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-c16c5a65-b641e4056cc6cb0eeEXAMPLE",
```

```
        "logged_time": 1668816977134,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-19T00:10:20.842295Z",
    "proxy": {
        "ip": "192.168.144.62",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-2f80f37e64EXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "10.14.173.3",
        "port": 55706
    },
    "start_time": "1668816620814",
    "status_code": "100",
    "status_details": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "20800101",
    "type_name": "AccessLogs: Access Granted",
    "unmapped": null
}
```


Acesso negado devido à falta de um cookie

Neste exemplo de entrada de log, o Acesso Verificado nega o acesso devido à falta de um cookie de autenticação.


```
{
    "activity": "Access Denied",
    "activity_id": "2",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": null,
```

```
    "duration": "0.0",
    "end_time": "1668593568259",
    "time": "1668593568259",
    "http_request": {
        "http_method": "POST",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/dns-query",
            "port": 443,
            "scheme": "h2",
            "text": "https://hello.app.example.com:443/dns-query"
        },
        "user_agent": "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML",
        "version": "HTTP/2.0"
    },
    "http_response": {
        "code": 302
    },
    "identity": null,
    "message": "",
    "metadata": {
        "uid": "Root=1-5cf1c832-a565309ce20cc7dafEXAMPLE",
        "logged_time": 1668593776720,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T10:12:48.259762Z",
    "proxy": {
        "ip": "192.168.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-108ed7a672EXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "10.7.178.16",
        "port": "46246"
    },
    "start_time": "1668593568258",
    "status_code": "200",
```

```
    "status_details": "Authentication Denied",
    "status_id": "2",
    "status": "Failure",
    "type_uid": "20800102",
    "type_name": "AccessLogs: Access Denied",
    "unmapped": null
}
```

Acesso negado pela política

Neste exemplo de entrada de log, o Acesso Verificado nega uma solicitação autenticada porque a solicitação não é permitida pelas políticas de acesso.

```
{
    "activity": "Access Denied",
    "activity_id": "2",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": {
        "ip": "10.4.133.137",
        "type": "Unknown",
        "type_id": 0
    },
    "duration": "0.023",
    "end_time": "1668573630978",
    "time": "1668573630978",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "h2",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36",
        "version": "HTTP/2.0"
    },
    "http_response": {
        "code": 401
```

```
    },
    "identity": {
        "authorizations": [],
        "idp": {
            "name": "user",
            "uid": "vatp-e048b3e0f8EXAMPLE"
        },
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "0e1281ad3580aEXAMPLE"
        }
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-531a036a-09e95794c7b96aefbEXAMPLE",
        "logged_time": 1668573773753,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T04:40:30.978732Z",
    "proxy": {
        "ip": "3.223.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-021d5eaed2EXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "10.4.133.137",
        "port": "31746"
    },
    "start_time": "1668573630955",
    "status_code": "300",
    "status_details": "Authorization Denied",
    "status_id": "2",
    "status": "Failure",
    "type_uid": "20800102",
    "type_name": "AccessLogs: Access Denied",
```

```
    "unmapped": null
}
```

Entrada de log desconhecida

Neste exemplo de entrada de log, o Acesso Verificado não pode gerar uma entrada de log completa, então emite uma entrada de log desconhecida. Isso garante que todas as solicitações apareçam no log de acesso.

```
{
    "activity": "Unknown",
    "activity_id": "0",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": null,
    "duration": "0.004",
    "end_time": "1668580207898",
    "time": "1668580207898",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "https",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "python-requests/2.28.1",
        "version": "HTTP/1.1"
    },
    "http_response": {
        "code": 200
    },
    "identity": null,
    "message": "",
    "metadata": {
        "uid": "Root=1-435eb955-6b5a1d529343f5adaEXAMPLE",
        "logged_time": 1668580579147,
        "version": "0.1",
        "product": {
            "name": "Verified Access",
```

```
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T06:30:07.898344Z",
    "proxy": {
        "ip": "10.1.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-6c32b53b3cEXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "172.28.57.68",
        "port": "47220"
    },
    "start_time": "1668580207893",
    "status_code": "000",
    "status_details": "Unknown",
    "status_id": "0",
    "status": "Unknown",
    "type_uid": "20800100",
    "type_name": "AccessLogs: Unknown",
    "unmapped": null
}
```


OCSFexemplos de log da versão 1.0.0-rc.2 para acesso verificado

Veja a seguir exemplos de registros usando a OCSF versão de registro 1.0.0-rc.2.

Conteúdo

Acesso concedido com contexto de confiança incluído


```
{
    "activity_name": "Access Grant",
    "activity_id": "1",
    "actor": {
        "authorizations": [{
```

```
            "decision": "Allow",
            "policy": {
                "name": "inline"
            }
        }],
        "idp": {
            "name": "user",
            "uid": "vatp-09bc4cbce2EXAMPLE"
        },
        "invoked_by": "",
        "process": {},
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "00u6wj48lbxTAEXAMPLE"
        },
        "session": {}
    },
    "category_name": "Audit Activity",
    "category_uid": "3",
    "class_name": "Access Activity",
    "class_uid": "3006",
    "device": {
        "ip": "10.2.7.68",
        "type": "Unknown",
        "type_id": 0
    },
    "duration": "0.004",
    "end_time": "1668580194344",
    "time": "1668580194344",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "https",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "python-requests/2.28.1",
        "version": "HTTP/1.1"
    },
    "http_response": {
```

```
        "code": 200
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-63748362-6408d24241120b942EXAMPLE",
        "logged_time": 1668580281337,
        "version": "1.0.0-rc.2",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T06:29:54.344948Z",
    "proxy": {
        "ip": "192.168.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-002fa341aeEXAMPLE"
    },
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "172.24.57.68",
        "port": "48234"
    },
    "start_time": "1668580194340",
    "status_code": "100",
    "status_detail": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "300601",
    "type_name": "Access Activity: Access Grant",
    "data": {
        "context": {
            "oidc": {
                "family_name": "Last",
                "zoneinfo": "America/Los_Angeles",
                "exp": 1670631145,
                "middle_name": "Middle",
                "given_name": "First",
                "email_verified": true,
                "name": "Test User Display",
                "updated_at": 1666305953,
                "preferred_username": "johndoe-user@test.com",
```

```
                "profile": "http://www.example.com",
                "locale": "US",
                "nickname": "Tester",
                "email": "johndoe-user@test.com"
            },
            "http_request": {
                "x_forwarded_for": "1.1.1.1,2.2.2.2",
                "http_method": "GET",
                "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36",
                "port": "80",
                "hostname": "hostname.net"
            }
        }
    }
}
```

Acesso concedido com contexto de confiança omitido

```
{
    "activity_name": "Access Grant",
    "activity_id": "1",
    "actor": {
        "authorizations": [{
            "decision": "Allow",
            "policy": {
                "name": "inline"
            }
        }],
        "idp": {
            "name": "user",
            "uid": "vatp-09bc4cbce2EXAMPLE"
        },
        "invoked_by": "",
        "process": {},
        "user": {
            "email_addr": "johndoe@example.com",
            "name": "Test User Display",
            "uid": "johndoe@example.com",
            "uuid": "00u6wj48lbxTAEXAMPLE"
        },
        "session": {}
    },
```

```
    "category_name": "Audit Activity",
    "category_uid": "3",
    "class_name": "Access Activity",
    "class_uid": "3006",
    "device": {
        "ip": "10.2.7.68",
        "type": "Unknown",
        "type_id": 0
    },
    "duration": "0.004",
    "end_time": "1668580194344",
    "time": "1668580194344",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "hello.app.example.com",
            "path": "/",
            "port": 443,
            "scheme": "https",
            "text": "https://hello.app.example.com:443/"
        },
        "user_agent": "python-requests/2.28.1",
        "version": "HTTP/1.1"
    },
    "http_response": {
        "code": 200
    },
    "message": "",
    "metadata": {
        "uid": "Root=1-63748362-6408d24241120b942EXAMPLE",
        "logged_time": 1668580281337,
        "version": "1.0.0-rc.2",
        "product": {
            "name": "Verified Access",
            "vendor_name": "AWS"
        }
    },
    "ref_time": "2022-11-16T06:29:54.344948Z",
    "proxy": {
        "ip": "192.168.34.167",
        "port": 443,
        "svc_name": "Verified Access",
        "uid": "vai-002fa341aeEXAMPLE"
    },
```

```
    "severity": "Informational",
    "severity_id": "1",
    "src_endpoint": {
        "ip": "172.24.57.68",
        "port": "48234"
    },
    "start_time": "1668580194340",
    "status_code": "100",
    "status_detail": "Access Granted",
    "status_id": "1",
    "status": "Success",
    "type_uid": "300601",
    "type_name": "Access Activity: Access Grant",
    "data": null
}
```


Registre API chamadas de acesso verificado usando AWS CloudTrail

AWS O Acesso Verificado é integrado com AWS CloudTrail um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um Serviço da AWS no Acesso Verificado. CloudTrail captura todas as API chamadas para acesso verificado como eventos. As chamadas capturadas incluem chamadas do console de Acesso Verificado e chamadas de código para as API operações de Acesso Verificado. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para acesso verificado. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao Verified Access, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

Informações de acesso verificadas em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no Acesso verificado, essa atividade é registrada em um CloudTrail evento junto com outros Serviço da AWS eventos no histórico de eventos. É possível visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em seu Conta da AWS, incluindo eventos para acesso verificado, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros Serviços da AWS para analisar e agir com base nos dados do evento coletados nos CloudTrail registros. Para obter mais informações, consulte as informações a seguir.

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando SNS notificações da Amazon para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas as ações de acesso verificado são registradas CloudTrail e documentadas na Amazon EC2 API Reference. Por exemplo, chamadas para o `CreateVerifiedAccessInstance` `DeleteVerifiedAccessInstance` e `ModifyVerifiedAccessInstance` as ações geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com as credenciais do usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro Serviço da AWS.

Para obter mais informações, consulte o CloudTrail userIdentity elemento.

Compreenda as Entradas dos arquivos de log do Acesso Verificado

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma solicitação única de qualquer fonte. Ele inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim

por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das API chamadas públicas, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro para a `CreateVerifiedAccessInstance` ação.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIKK4OOINJWEXAMPLE:jdoe",
        "arn": "arn:aws:iam::123456789012:user/jdoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "jdoe"
    },
    "eventTime": "2022-11-18T20:44:04Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateVerifiedAccessInstance",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "CreateVerifiedAccessInstanceRequest": {
            "Description": "",
            "ClientToken": "85893b1e-49f6-4d24-97de-280c664edf1b"
        }
    },
    "responseElements": {
        "CreateVerifiedAccessInstanceResponse": {
            "verifiedAccessInstance": {
                "creationTime": "2022-11-18T20:44:04",
                "description": "",
                "verifiedAccessInstanceId": "vai-0d79d91875542c549",
                "verifiedAccessTrustProviderSet": ""
            },
            "requestId": "2eae195d-6bfd-46d7-b46e-a68cb791de09"
        }
    },
    "requestID": "2eae195d-6bfd-46d7-b46e-a68cb791de09",
    "eventID": "297d6529-1144-40f6-abf8-3a76f18d88f0",
    "readOnly": false,
    "eventType": "AwsApiCall",
```

```
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Cotas para Acesso Verificado pela AWS

Você Conta da AWS tem cotas padrão, anteriormente chamadas de limites, para cada um. Serviço da AWS A menos que especificado de outra forma, cada cota é específica da região.

Cotas de nível da Conta da AWS

Você Conta da AWS tem as seguintes cotas relacionadas ao Acesso Verificado.

Nome	Padrão	Ajustável	Descrição
Instâncias de Acesso Verificado	5	Sim	O número máximo de instâncias de Acesso Verificado que podem ser criadas pelos clientes na região atual.
Grupos de Acesso Verificado	10	Sim	O número máximo de grupos de Acesso Verificado que podem ser criados pelos clientes na região atual.
Provedores de confiança de Acesso Verificado	15	Sim	O número máximo de provedores confiáveis de Acesso Verificado que podem ser criados pelos clientes na região atual.
Endpoints de Acesso Verificado	50	Sim	O número máximo de endpoints de Acesso Verificado que podem ser criados pelos clientes na região atual.

HTTPcabeçalhos

A seguir estão os limites de tamanho dos HTTP cabeçalhos.

Nome	Padrão	Ajustável
Linha de solicitação	16 K	Não
Cabeçalho único	16 K	Não
Cabeçalho de resposta inteiro	32 K	Não
Cabeçalho da solicitação inteira	64 K	Não

OIDCtamanho da reclamação

A seguir está o limite de tamanho da OIDC reclamação.

Nome	Padrão	Ajustável
OIDCtamanho da reclamação	11 K	Não

Histórico do documento para o guia do usuário do Acesso Verificado

A tabela a seguir descreve as versões de documentação para o Acesso Verificado.

Alteração	Descrição	Data
AWS política gerenciada atualizada	Atualização feita na IAM política AWS gerenciada para acesso verificado.	17 de novembro de 2023
Criptografia de dados em repouso	AWS O Verified Access criptografa dados em repouso por padrão, usando KMS chaves AWS próprias.	28 de setembro de 2023
Support para FIPS conformidade	Configure o acesso verificado para fins de FIPS conformidade.	26 de setembro de 2023
Registro em log aprimorado	Adição do recurso de log que adiciona contextos de confiança aos logs.	19 de junho de 2023
AWS política gerenciada atualizada	Atualização feita na IAM política AWS gerenciada para acesso verificado.	31 de maio de 2023
Lançamento do GA	Versão GA do Guia do Usuário do Acesso Verificado. Inclui a integração AWS WAF.	27 de abril de 2023
Versão de visualização	Versão prévia do Guia do usuário do Acesso Verificado	29 de novembro de 2022

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.